I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Protecting the Nation's Cyber Infrastructure: Is the Department of Homeland Security Our Nation's Savior or the Albatross Around Our Neck?

REBECCA C.E. MCFADYEN*

Abstract: For centuries, the defense of this nation has focused on the protection of its physical infrastructure. Now, in the Digital age, this nation must also focus on the protection of its cyber infrastructure. Attacks on both the private and public sectors are constant and costly. The federal government has tasked the Department of Homeland Security with the protection of the nation's cybersecurity. However, the young Department has struggled to define itself as a leader in this industry. This article explores the formation of the Department and its well-chronicled leadership, management, and credibility woes.

* The author graduated from the College of the Holy Cross (B.A. 1998) and from the University of Florida (Ph.D. 2004, J.D. 2007). The author would like to thank her husband, whose patience and understanding allow the author to pursue all her passions.

"Our enemies are innovative and resourceful, and so are we. They never stop thinking about new ways to harm our country and our people, and neither do we."[1]

I. INTRODUCTION

Sit down, close your eyes, take a deep breath, and then imagine.

> Imagine the lights in this room suddenly go out, and we lose all power. We try to use our cell phones, but the lines of communication are dead. We try to access the Internet with our battery-powered laptops, but the Internet, too, is down. After a while, we venture out into the streets to investigate if this power outage is affecting more than just our building, and the power is indeed out as far as the eye can see. A passer-by tells us the banks are closed and the ATMs aren't working. The streets are jammed because the traffic lights are out, and people are trying to leave their workplaces en masse. Day turns to night, but the power hasn't returned. Radio and TV stations aren't broadcasting. The telephone and Internet still aren't working, so there's no way to check in with loved ones. After a long, restless night, morning comes, but we still don't have power or communication. People are beginning to panic, and local law enforcement can't restore order. As another day turns to night, looting starts, and the traffic jams get worse. Word begins to spread that the US has been attacked– not by a conventional weapon, but by a cyber weapon. As a result, our national power grid, telecommunications, and financial systems have been disrupted– worse yet, they won't be back in a few hours or days, but in months. The airports and train stations have closed. Food production has ceased. The water supply is rapidly deteriorating. Banks are closed so people's life savings are out of reach and worthless. The only things of value now are gasoline, food and

---

[1] George W. Bush, President of the United States of America, Remarks by the President at the Signing of H.R. 4613, the Defense Appropriations Act for Fiscal Year 2005 (Aug. 5, 2004).

> water, and firewood traded on the black market. We've gone from being a superpower to a third-world nation practically overnight.[2]

There was a time when people believed that the Atlantic Ocean to the East and the Pacific Ocean to the West protected the United States from a physical attack. Pearl Harbor, and more recently, September 11, 2001, changed that perspective. The 9/11 terrorist attacks forced the United States to re-evaluate its physical security. While "the emphasis has clearly been on physical infrastructure rather than cybersecurity," the Digital Age arrived and "cyberspace is where the bad guys are going."[3] Any re-evaluation of national security must necessarily focus on the Nation's cyber infrastructure. Geographic isolation no longer provides any protection, because "[i]n cyberspace national boundaries have little meaning. Information flows continuously and seamlessly across political, ethnic, and religious divides . . . ."[4]

II. THE DEPARTMENT OF HOMELAND SECURITY IS BORN

The vast interconnectedness of cyberspace provides nearly instant access to incredible amounts of information. That access to information changed the course of ordinary business, the availability of an education, and the way people interact. This interconnectedness is not without significant risks as the "vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them."[5]

---

[2] *Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology of the H. Comm. on Homeland Security*, 110th Cong. (2007) (statement of O. Sami Saydjari, President, Professionals for Cyber Defense, and Chief Executive Officer, Cyber Defense Agency, LLC) [hereinafter *Reducing Vulnerabilities*], *available at* http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf.

[3] Jon Swartz, *Terrorists' use of Internet spreads*, USA TODAY, Feb. 21, 2005, http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm.

[4] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 7 (2003), http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

[5] *Id.*

"Given the ever evolving nature of cyberthreats, complacency is not an option."[6] After the terrorist attacks of September 11, 2001, the federal government responded, in part, by melding twenty-two existing federal organizations and agencies into one new department– the Department of Homeland Security ("the Department").[7] The government had not attempted a "transformation of this magnitude" since the 1940s when the government created the Department of Defense.[8] By consolidating the responsibilities of these twenty-two component agencies, this "ambitious undertaking" labored to improve the nation's preparedness.[9] Because "[c]ritical infrastructure is by definition essential for the survival of the nation [and] [n]etworked computer systems form the nerve center of the country's critical infrastructure," the government's preparedness efforts also includes efforts to secure the nation's cyber infrastructure. The Department describes its "overriding and urgent mission" as securing the American homeland and protecting the American people.[10]

In the years following its inspired inception, the Department has faltered. "Contracting abuses, poor leadership, and low employee moral" have plagued the Department.[11] Regarding the Department's programs, personnel, and resources, government reports continuously document the Department's "[i]nadequate staffing, insufficient

---

[6] Daniel Pullman, *GAO Again Slams Agencies' Cybersecurity Efforts*, GOV'T EXECUTIVE, July 19, 2005 (statement of Representative Tom Davis, R-VA, Chairman of the H. Comm. on Oversight and Government Reform), www.govexec.com/story_page.cfm?articleid=31778.

[7] H. COMM. ON HOMELAND SEC., CRITICAL LEADERSHIP VACANCIES IMPEDE U.S. DEPARTMENT OF HOMELAND SECURITY 1 (2007) [hereinafter CRITICAL LEADERSHIP VACANCIES], http://homeland.house.gov/SiteDocuments/20070709112923-81091.pdf.

[8] U.S. GEN. ACCOUNTABILITY OFFICE, DEPARTMENT OF HOMELAND SECURITY: FINANCIAL MANAGEMENT CHALLENGES 1 (2004), *available at* http://www.gao.gov/new.items/d04945t.pdf.

[9] CRITICAL LEADERSHIP VACANCIES, *supra* note 7.

[10] DEPT. OF HOMELAND SEC., SECURING OUR HOMELAND 2 (2004), http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf. The Department's strategic goals and objectives are directly linked to accomplishing the three objectives of the President's National Strategy for Homeland Security: (1) prevent terrorist attacks from occurring within the United States, (2) reduce America's vulnerability to terrorism; and (3) minimize the damage of such attacks and improve the recovery process from those attacks that do occur.

[11] Pullman, *supra* note 6.

training, and ineffective monitoring." [12] These weaknesses are particularly conspicuous in the context of the Department's efforts to secure the nation's cyber infrastructure. For instance, the Department initially failed to properly accord the nation's cyber infrastructure the attention and resources required for its protection. To some extent, the Department self-corrected, and eventually, after a fourteen-month delay, named an Assistant Secretary of Cybersecurity.[13] Nevertheless, the Department suffered a massive exodus of key cybersecurity officials.[14] Furthermore, the palpable tension between Congress and the Department undermines the government's ability to protect the nation's cyber infrastructure. Because such protection requires "swift and ongoing decision making, often based on gut-feeling, rather than on what the text book dictates,"[15] the fundamental question is can the Department get the job done?

Every minute of every hour of every day, the nation's cyber infrastructure is under attack. The increases in the frequency and the complexity of cyber attacks are alarming.[16] Such cyber attacks range from relatively minor acts including cyber vandalism and theft of intellectual property, to more serious crimes such as extortion, industrial espionage, and the stoppage of production and services.[17]

---

[12] U.S. GEN. ACCOUNTABILITY OFFICE, PURCHASE CARDS: CONTROL WEAKNESSES LEAVE DHS HIGHLY VULNERABLE TO FRAUDULENT, IMPROPER, AND ABUSIVE ACTIVITY 11 (2006), *available at* http://www.gao.gov/new.items/d061117.pdf.

[13] Declan McCullagh, *Homeland Security fills top cybersecurity post*, CNET NEWS, Sept.18, 2006, http://news.cnet.com/Homeland-Security-fills-top-cybersecurity-post/2100-7348_3-6116975.html.

[14] Eric Lipton, *Former Anti-Terror Officials Find Industry Pays Better*, NEW YORK TIMES, June 18, 2006, http://www.nytimes.com/2006/06/18/washington/18lobby.html.

[15] KFIR DAMARI, AMI CHAYUN & GADI EVRON, CASE STUDY: A CYBER-TERRORISM ATTACK, ANALYSIS AND RESPONSE (2006), http://www.beyondsecurity.com/besirt/advisories/team-evil-incident.pdf.

[16] Larry Greenemeier, *China's Cyber Attacks Signal New Battlefield Is Online*, SCIENTIFIC AMER., Sept. 18, 2007, http://www.sciam.com/article.cfm?articleID=1A9C210F-E7F2-99DF-3C85F17B1680980D&sc=I100322.

[17] *Major Cyberspace Vulnerabilities Will Be Used Against Us: Hearing Before H. Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the H. Comm. on Oversight and Government Reform*, 108th Cong. (2003) (statement of Richard Clark, Special Advisor, United States National Security Council) [hereinafter *Major Cyberspace Vulnerabilities*], *available at* http://www.au.af.mil/au/awc/awcgate/congress/clarke_8apr03.pdf.

The Federal Bureau of Investigation ("FBI") described cyber terrorism as a "criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."[18] Because the United States is specifically "vulnerable to a strategically crippling cyber attack from nation-state-class adversaries . . . the government must *provide for the common defense* of this new territory."[19]

As current Assistant Secretary of Cybersecurity and Communications Greg Garcia explained, "300 million Americans count on us every day for uncompromised continuity of operations of our most critical systems, such as financial services, transportation, government and emergency services, online commerce, health care, manufacturing, and process control systems like water purification and electric power plants."[20] In short, America can no longer afford to turn a blind eye to the dangers lurking in cyberspace. Experts agree that it is "unreasonable to think that even the nation's most secure critical networks are impervious to attacks," and that it is absolutely crucial for the U.S. to have networks that can provide "essential services in a timely manner despite an attack, accident, or failure."[21] Securing the nation's cyber infrastructure must be an indispensable national priority. Hence, in conjuction with other important goals, the federal government created the Department of Homeland Security.

On November 25, 2002, President George W. Bush signed into law the legislation that created the Department of Homeland Security. The Homeland Security Act charged the Department with three

---

[18] *Virtual Threat, Real Terror: Cyberterrorism in the 21st Century: Hearing Before the S. Subcomm. on Terrorism, Technology, and Homeland Security of the S. Comm. on the Judiciary*, 108th Cong. (2004) (statement of Keith Lourdeau, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation), *available at* http://judiciary.senate.gov/print_testimony.cfm?id=1054&wit_id=2995.

[19] *Reducing Vulnerabilities, supra* note 2.

[20] Gregory Garcia, Remarks at the Third Annual Government Forum of Incident Response and Security Teams Conference (June 26, 2007), *available at* http://www.dhs.gov/xabout/gc_1182960010006.shtm.

[21] Press Release, American Association for the Advancement of Science, Internet Security Experts Urge U.S. to Secure its Critical Computer Networks (June 8, 2007), *available at* http://www.aaas.org/news/releases/2007/0608cybersec.shtml (statement of Howard Lipson).

primary strategic objectives.[22] To accomplish these objectives, the bill organized the Department into four different directorates, which included (1) Border and Transportation Security, (2) Emergency Preparedness and Response, (3) Science and Technology, and (4) Information Analysis and Infrastructure Protection.[23]

The development of this new executive department was an ambitious undertaking. "Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. Each of the 22 agencies and organizations brought their own management challenges, distinct missions, unique information technology infrastructures and systems."[24] The twenty-two new components of the Department included Immigration and Customs Enforcement ("ICE"), the Transportation Security Administration ("TSA"), the Federal Emergency Management Agency ("FEMA"), the Nuclear Incident Response Team, the Plum Island Animal Disease Center, the Federal Computer Incident Response Center, the Secret Service, and the Coast Guard.[25] While, on January 1, 2003, the Department technically became a functional part of the federal government, the Department did not assume the responsibilities of most of its assimilated twenty-two agencies and organizations until March 2003.

A. THE DEPARTMENT ENTERS THE CYBER SECURITY SCENE

Among its numerous responsibilities, the Department of Homeland Security is also the nation's top cybersecurity watchdog. After the Department's creation, President Bush eliminated the position of Senior Advisor to the President on Cybersecurity. Consequently, federal law and policy delegated to the Department thirteen key cybersecurity-related responsibilities.[26] These thirteen responsibilities obligate the Department to:

---

[22] Homeland Security Act of 2002, Pub. L. No. 107-296 (2002).

[23] Department of Homeland Security, History: Who Became Part of the Department? [hereinafter DHS History], http://www.dhs.gov/xabout/history/editorial_0133.shtm.

[24] U.S. GEN. ACCOUNTABILITY OFFICE, INFORMATION SECURITY: HOMELAND SECURITY NEEDS TO ENHANCE EFFECTIVENESS OF ITS PROGRAM 3 (2007), *available at* http://www.gao.gov/new.items/d071003t.pdf.

[25] DHS History, *supra* note 23.

[26] Zoe Lofgren, *Perspective: Thumb Twiddling on Cybersecurity*, CNET NEWS, Oct. 10, 2004, http://www.news.com/2010-7348_3-5420059.html.

1. develop a national plan to provide protection for the nation's critical infrastructure, including its cyber infrastructure,

2. develop partnerships with other federal agencies, state and local governments, and the private sector,

3. improve the process by which the government and the private sector share information regarding cyber attacks, threats, and vulnerabilities,

4. develop the process by which the government issues warnings regarding cyber threats and attacks,

5. coordinate the government's response and recovery planning efforts following a cyber attack,

6. identify and evaluate cyber threats and vulnerabilities,

7. support efforts to reduce cyber threats and vulnerabilities,

8. promote research and development efforts to strengthen the nation's cyber infrastructure,

9. promote awareness regarding cybersecurity issues,

10. foster cybersecurity training and certification,

11. enhance the cybersecurity of federal, state, and local governments,

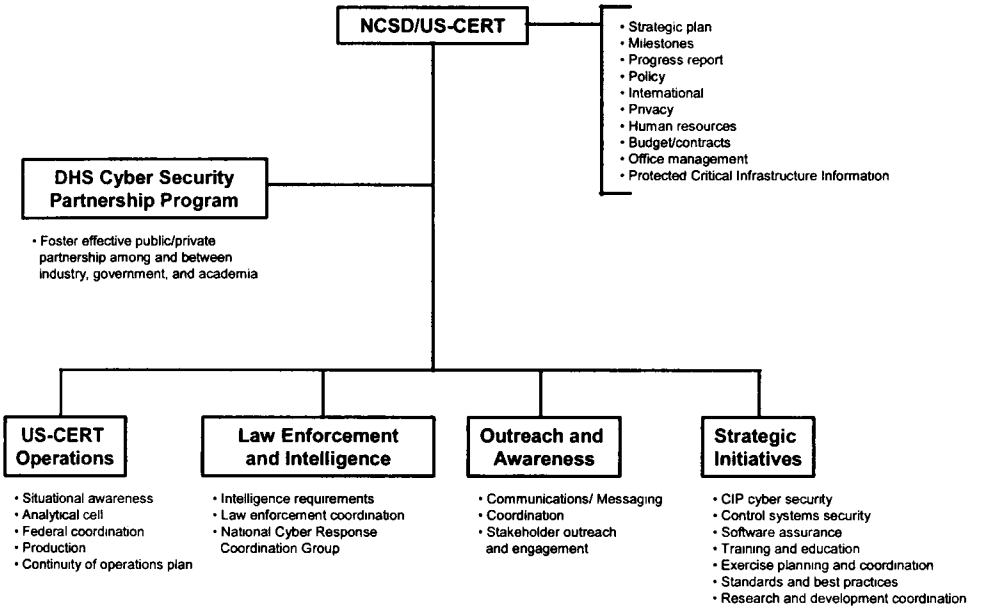
12. strengthen international cyberspace security, and

13. integrate cybersecurity with national security.[27]

---

[27] *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity, Hearing Before the S. Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs*, 109th Cong. (2005) (statement of David A. Powner, Director, Information Technology Management Issues), *available at* http://www.gao.gov/new.items/d05827t.pdf.

In June 2003, the Department established the National Cyber Security Division ("NCSD") to serve as the national focal point for addressing cybersecurity-related issues and coordinating the implementation of the government's cybersecurity efforts.[28] Four separate branches as well as a public/private cybersecurity partnership program comprise the NCSD. This collaboration facilitates partnerships between the Department and other interested industrial, governmental, and academic parties.[29] The organizational chart for NCSD is provided below.



Each of the four NCSD branches has several responsibilities. The US-CERT Operations Branch "focuses on situational awareness, analytical cells, and federal coordination." To this end, the operations branch coordinates all cyber incidents warnings and responses across both the government and the private sector . . . ."[30] US-CERT is always operational.[31] The Law Enforcement and Intelligence Branch

---

[28] U.S. GOV. ACCOUNTABILITY OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: DEPARTMENT OF HOMELAND SECURITY FACES CHALLENGES IN FULFILLING CYBERSECURITY RESPONSIBILITIES 2 (2005) [hereinafter CRITICAL INFRASTRUCTURE PROTECTION], *available at* http://www.gao.gov/new.items/d05434.pdf.

[29] *Id.* at 24.

[30] *Id.* at 25.

[31] *Id.* at 26.

manages the National Cyber Response Coordinating Group and facilitates the coordination of NCSD's cyber-related law enforcement and intelligence activities.[32] The Outreach and Awareness Branch strives to promote cybersecurity awareness,[33] and works to develop collaborative cybersecurity partnerships between public and private entities.[34] Lastly, the Strategic Initiatives Branch is organized into six different teams with each team maintaining different functional responsibilities. The responsibilities of this branch include (1) developing a critical infrastructure protection plan for the Information Technology ("IT") Sector,[35] (2) promoting the development of an adequate number of effective cybersecurity professionals, (3) enhancing the cybersecurity capability of the government's work force,[36] and (4) improving the nation's ability to respond to cyber incidents.[37]

B. THE NATION'S REVOLVING DOOR OF CYBERSECURITY LEADERSHIP

A series of high profile resignations underscores the nation's cybersecurity leadership woes. Before the Department became functional in January 2003, Richard Clarke held the nation's top cybersecurity position as Chairman of the President's Critical Infrastructure Protection Board ("CIPB").[38] As the momentum behind the Department's formation increased, Clarke jockeyed for the position of Deputy Secretary under the Department's first Secretary,

---

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.* at 27.

[36] *Id.*

[37] *Id.* at 27–28.

[38] Robert O'Harrow Jr. & Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, http://www.washingtonpost.com/wp-dyn/articles/A64915-2004Oct1.html. On October 19, 2001, President George W. Bush announced that he had designated Richard Clarke as Chair of the President's Critical Infrastructure Protection Board. At the time of this appointment, Clarke also served as the Special Advisor to the President for Cyber Space Security.

Tom Ridge.[39] Clarke allegedly vocalized that he would not accept any position other than that of the Deputy Secretary.[40] But, after President Bush did not select Clarke as Deputy Secretary of the Department, a White House spokesperson noted that a slighted Clarke boycotted the National Security Council meetings then chaired by Condoleezza Rice.[41] Finally, on January 30, 2003, Clarke resigned as Chairman.[42]

Following Clarke's resignation, Howard A. Schmidt, who had previously served as Vice-Chairmain of the CIPB, became the front-runner for the nation's top cybersecurity advisor.[43] After the February 2003 release of the *National Strategy to Secure Cyberspace*, however,

---

[39] Interview by Larry King with Richard Clarke, former White House advisor (Mar. 24, 2004), transcript *available at* http://transcripts.cnn.com/TRANSCRIPTS/0403/24/lkl.00.html. During the interview, Condoleezza Rice, then-National Security Advisor stated:

> In fact, when he came to me and asked if I would support him with Tom Ridge to become the deputy secretary of homeland security, a department which he now says should never have been– never have been created. When he asked me to support him in that job, he said he supported the president. So frankly, I'm flabbergasted.

Interview by Tim Russert with Richard Clarke, former White House counterterrorism official (Mar. 28, 2004), transcript *available at* http://www.msnbc.msn.com/id/4608698. Moderator Tim Russert stated:

> One article captured it this way: 'Mr. Clarke . . . who had sought the No. 2 spot at Homeland Security, was passed over for the post in October 2002 and demoted by Secretary Tom Ridge and National Security Adviser Condoleezza Rice to the position of special adviser for cyberspace security.'

[40] Barton Gellman, *Anti-Terror Pioneer Turns In the Badge*, WASH. POST, Mar. 13, 2003, at A21, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A17694-2003Mar12.

[41] J. Michael Waller, *Clarke's Colleagues Say He's Lost Credibility*, WORLD NET DAILY, Mar. 30, 2004, http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=37790.

[42] Associated Press, *U.S. Cybersecurity Czar to Resign*, WIRED, Jan. 28, 2003, http://www.wired.com/politics/law/news/2003/01/57454.

[43] Dan Verton, *Howard Schmidt Leaving Government Cybersecurity Job*, COMPUTERWORLD, Apr. 21, 2003, http://www.computerworld.com/securitytopics/security/story/0,10801,80549,00.html. On January 28, 2002, Schmidt, assumed his role as Vice-Chairman of the Critical Infrastructure Protection Board. *See* Dan Verton, *Former Microsoft Exec Begins Federal Critical Infrastructure Protection Job*, COMPUTERWORLD, Jan. 28, 2002, http://www.computerworld.com/securitytopics/security/story/0,10801,67754,00.html.

the President dissolved the CIPB and shifted to the Department the responsibilities of securing the nation's cyber infrastructure.[44] Just three months after Clarke's resignation—possibly sensing that his role in the nation's cybersecurity leadership was tenuous—Schmidt resigned. [45] In an April 21, 2003 resignation e-mail, Schmidt explained:

> [w]hile significant progress has been made, there still is much to do. It is the role of industry to take the lead in the implementation of the strategy and the creation of the mosaic of security. To accomplish this will require real-time solutions, not just reports and plans that take years to implement [and] have limited value in dealing with the tremendous vulnerabilities that exist here and now. Each sector, each enterprise, each company and each user must do their part to secure their piece of cyberspace.[46]

The resignations of Clarke and Schmidt left the government without a cybersecurity point person. As one industry official lamented, "[c]urrently, no one's in charge. You have no effective advocate whose only job is to focus on cybersecurity."[47] Consequently, the responsibility of overseeing the nation's cybersecurity fell onto the shoulders of the Department's Assistant Secretary for Infrastructure Protection, then Robert Liscouski. [48] As Assistant Secretary, Liscouski's responsibilities were already expansive and included the

---

[44] William Jackson, *Howard Schmidt is Leaving the White House*, GOV'T COMPUTER NEWS, Apr. 21, 2003, http://www.gcn.com/online/vol1_no1/21815-1.html.

[45] Margaret Kane, *White House Security Adviser Resigns*, CNET NEWS, Apr. 22, 2003, http://www.news.com/White-House-security-adviser-resigns/2100-1009_3-997840.html. On October 19, 2001, President George W. Bush announced that he had designated Richard Clarke as Chair of the President's Critical Infrastructure Protection Board. At the time of this appointment, Clarke also served as the Special Advisor to the President for Cyber Space Security.

[46] Verton, *supra* note 43; *see also* Jackson, *supra* note 44 (noting that Schmidt reportedly sought a position as adviser to the Secretary Ridge).

[47] Caron Carlson, *Departures Cast Doubt on IT Security at DHS*, EWEEK, Apr. 28, 2003, http://www.eweek.com/c/a/Security/Departures-Cast-Doubt-on-IT-Security-at-DHS.

[48] *Id.*

protection of both the nation's physical and virtual infrastructures.[49] Consequently, critics complained that neither the White House nor the Department had a high-ranking official whose duties were exclusively dedicated to protecting the nation's cybersecurity.[50]

C. THE DEPARTMENT FINALLY ADDRESSES CYBERSECURITY LEADERSHIP

Later that year, the Department attempted to address the void in its cybersecurity leadership. On September 15, 2003, Secretary Ridge announced the appointment of Amit Yoran as the Director of NCSD.[51] Yoran's appointment pleased the Business Software Alliance ("BSA"). Robert Holleyman, BSA's President and Chief Executive Officer, explained that "Mr. Yoran has worked extensively in the public and private sectors to prevent and respond to information security breaches. He knows first hand the vast threats that exist today and what needs to be done to quickly identify, assess, and mitigate those threats."[52]

During testimony at a Congressional hearing, titled *Virtual Threat, Real Terror: Cyberterrorism in the 21st Century*, Yoran explained that NCSD serves as the focal point for "[e]nhancing the Nation's cyber readiness and response, analyzing cyber threats and vulnerabilities, disseminating threat warning information through alerts and warnings, [and] coordinating incident response." [53]

---

[49] *Id.*

[50] Jackson, *supra* note 44.

[51] Press Release, Tom Ridge, Secretary of Homeland Security Tom Ridge Announces Director of the National Cyber Security Division (Sept. 15, 2003), *available at* http://www.dhs.gov/xnews/releases/press_release_0242.shtm. According to the Press Release, Yoran served as the Vice President for Managed Security Services at Symantec Corporation. Prior to his move to the private sector, Yoran was the Director of the Vulnerability Assessment Program within the Computer Emergency Response Team at the Department of Defense, and the Network Security Manager at the Department of Defense. In this position, Yoran was responsible for maintaining operations of the Pentagon's network.

[52] *Amit Yoran Named Head of Cyber Security Division*, TECH LAW JOURNAL DAILY E-MAIL ALERT, Sept 12, 2003, http://www.techlawjournal.com/alert/2003/09/16.asp.

[53] *Virtual Threat, Real Terror: Cyberterrorism in the 21st Century: Hearing Before the Subcomm. on Terrorism, Tech., and Homeland Security of the S. Comm. on the Judiciary*, 108th Cong. (2004) (statement of Amit Yoran, Director, National Cyber Security Division Department of Homeland Security), *available at*

According to Yoran, NCSD's top priorities were "to prevent a cyber attack from occurring and to limit its scope and impact on the critical infrastructures . . . ."[54] He continued, "[o]ur government has a fundamental duty to warn the public of imminent threats and to provide protective measures, or at least the information necessary for the public to protect their systems."[55] NCSD's initial attempt to provide to the public valuable cyber security information appeared successful. On January 28, 2003, the day that NCSD inaugurated the US-CERT web site, the US-CERT web site recorded more than one million hits.[56] Within days of its launch, more than 250,000 direct subscribers received national cyber alerts.[57]

Despite the appearance of progress, Yoran's position was still several levels removed from the Department's Secretary. At the time of Yoran's appointment, the Director of the NCSD reported to the Assistant Secretary for Infrastructure Protection of the Information Analysis and Infrastructure Protection Directorate (then Robert Liscouski). The Assistant Secretary then reported to the Under Secretary for Information Analysis and Infrastructure Protection. Finally, the Under Secretary reported to the Secretary of Homeland Security.[58]

In September 2004, just one year after his appointment, Yoran resigned from the nation's top cybersecurity position.[59] Yoran's abrupt departure prompted widespread speculation in the cybersecurity community. Although Yoran denied it, many in the industry believed that the Department disappointed Yoran by not providing him with enough authority to attack the nation's cybersecurity problems.[60] Consequently, "[t]here was a sense it was

---

http://judiciary.senate.gov/hearings/testimony.cfm?renderforprint=1&id=1054&wit_id=2998.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Amit Yoran Named Head of Cyber Security Division*, *supra* note 52.

[59] O'Harrow Jr. & McCarthy, *supra* note 38.

[60] *Id.* Regarding Yoran's departure, one industry source concluded that "[h]e's an entrepreneur who wanted to get things moving, and I think he finally got to the point where he realized he could be more effective working outside the government." Dan Verton, *Nation's Cybersecurity Chief Abruptly Quits DHS Post*, COMPUTERWORLD, Oct. 1,

essentially a powerless position."[61] In an interview following his departure, Yoran maintained that he "never applied for an assistant secretary position," and that he "never advocated for one."[62] Yoran explained that he resigned because "[t]he startup work was complete, so to speak. I helped craft a series of programs and initiatives, and recruited talented engineering expertise, so I decided it was time to move on."[63] Because the Department "made some tangible and tactical operational achievements, including establishing the US-CERT," Yoran felt comfortable leaving the Department at that time.[64] "We've mapped the government's entire IT space and made progress on control system security. So my departure wasn't quite as abrupt as some reports have indicated."[65]

Nevertheless, some considered Yoran's resignation another setback for national cyber security. Paul Kurtz, Executive Director of the Cyber Security Industry Alliance ("CSIA"), noted that Yoran's departure was "symptomatic of the frustration all around," and as a result of this resignation, "[c]yber-security has fallen down on that totem pole."[66] He continued, "The bottom line is that without an individual at a senior level in charge of cybersecurity at the DHS, the

---

2004, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=96369&pageNumber=1.

[61] O'Harrow Jr. & McCarthy, *supra* note 38. Goodall noted that as Yoran "was trying to elevate his priorities in the DHS, he had to do battle with the marketplace and the politics of the issue. I can empathize with the difficulty of trying to do that." *See* Verton, *supra* note 43.

[62] Robert Lemos, *U.S. Cybersecurity Chief Resigns*, CNET NEWS, Oct. 1, 2004, http://www.news.com/U.S.-cybersecurity-chief-resigns/2100-7348_3-5392501.html.

[63] Todd Datz, *Amit Yoran on Why He Left DHS*, CSO MAG., Apr. 1, 2005, http://www.csoonline.com/article/220223/Amit_Yoran_on_Why_He_Left_DHS?page=1

[64] *Id.*

[65] Verton, *supra* note 43. Following his departure, Yoran described his biggest frustration regarding the Department as:

> Perhaps a lack of effectiveness in much of the government's security practices, a lack of practicality. There's a phenomenal amount of paperwork around certification and accreditation. There's a significantly sized industry around Washington, D.C., running paperwork exercises on cybersecurity, as opposed to investing in improved operations and implementing security technologies.

[66] O'Harrow Jr. & McCarthy, *supra* note 38.

vision, priorities and programs are not coming together."[67] Douglas J. Goodall, Chief Executive of RedSiren, also saw Yoran's departure as a significant loss: "The fear that I would have is that [the] momentum he was building would go away. Now we start all over again. And the government's attention span is fleeting."[68] Similarly, cyber security specialist Kevin Poulsen explained that Yoran's resignation was merely a symptom of the more virulent condition. Simply stated, "[i]n an age of physical terrorism and real-world threat, [the Department is] not giving cyber-security much attention."[69] Then, just three months after Yoran's resignation as Director of the NSCD, Assistant Secretary for Infrastructure Protection Robert Liscouski also resigned.[70]

D. THE DEPARTMENT'S BIG ANNOUNCEMENT

Finally, on July 13, 2005, Homeland Security Secretary Michael Chertoff announced the Department's new six-point agenda.[71] "[D]esigned to ensure that the Department's policies, operations, and structures are aligned in the best way to address the potential threats—both present and future—that face our nation,"[72] the six-point agenda included several organizational initiatives. According to Secretary Chertoff, the "Department must drive improvement with a sense of urgency. Our enemy constantly changes and adapts, so we as a Department must be nimble and decisive."[73] The agenda renamed

---

[67] Jaikumar Vijayan, *Lack of Leadership Hampers Cybersecurity Efforts, Says Critics*, COMPUTERWORLD, Sept. 18, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=112820&intsrc=article_more_side.

[68] Verton, *supra* note 43.

[69] O'Harrow Jr. & McCarthy, *supra* note 38.

[70] Press Release, Department of Homeland Security, Statement by the Department of Homeland Security on Assistant Secretary Bob Liscouski's Resignation (Jan. 11, 2005), *available at* http://www.dhs.gov/xnews/releases/press_release_0593.shtm.

[71] Press Release, Department of Homeland Security, Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security (July 13, 2005), *available at* http://www.dhs.gov/xnews/releases/press_release_0703.shtm.

[72] *Id.*

[73] *Id.*

the Information Analysis and Infrastructure Protection Directorate as the Directorate for Preparedness, and by doing so, the agenda consolidated preparedness assets from across the Department's various components.[74] Managed by an Undersecretary, this new Directorate also formed another new position– the Assistant Secretary for Cyber Security and Telecommunications.[75] The agenda charged the new Assistant Secretary with "identifying and assessing the vulnerability of critical telecommunications infrastructure and assets; providing timely, actionable and valuable threat information; and leading the national response to cyber and telecommunications threats."[76]

Many praised Chertoff's announcement. As Symantec's government relations manager, Tiffany Jones said, "[t]he establishment of an assistant secretary for cybersecurity and telecommunications will be a tremendous asset for developing a coordinated, national approach needed to address the myriad of information security challenges that individuals and enterprises face today."[77] The Cyber Security Industry Alliance ("CSIA"), which had already asked for coordination and guidance from the Department, "commend[ed] Homeland Security Secretary Michael Chertoff and the Department of Homeland Security ("DHS") for their decision to create an Assistant Secretary for Cyber Security and Telecommunications."[78] But, CSIA President Kurtz cautioned that the creation of the new Assistant Secretary position was not a cure-all, but "certainly a significant first step in raising the level of importance of cyber security nationally. It creates the foundation needed to move forward with the execution of a comprehensive approach to cyber security that builds on public and private sector efforts to date."[79]

---

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] Anne Broache, *Feds Create New Post of Cybersecurity Czar*, ZDNET, July 13, 2005, *available at* http://news.zdnet.com/2100-1009-5787086.html. The Assistant Secretary for Cyber Security and Telecommunications: Renewed Leadership from DHS, EXECUTIVE DIRECTOR'S MESSAGE (Cyber Security Industry Alliance, Arlington, Va), July/August 2005 [hereinafter Renewed Leadership from DHS], *available at* https://www.csialliance.org/news/newsletters/july2005/july_execdir.html.

[78] Renewed Leadership from DHS, *supra* note 77.

[79] *Id.*

E. THE WAITING GAME

Despite the wave of excitement following Secretary Chertoff's announcement, the lengthy delay in actually appointing the Assistant Secretary curbed the industry's support for the Department's initiatives. The execution of this "significant first step" required much more time than the industry expected, prompting CSIA's Executive Director Kurtz to conclude that the absence of an assistant secretary was "not a simple personnel issue. It is indicative of the ongoing lack of attention being paid to cybersecurity at the most senior levels of government."[80] Kurtz's sentiment was clear: "The bottom line is that without an individual at a senior level in charge of cybersecurity at the DHS, the vision, priorities and programs are not coming together."[81]

Congressional irritation over the absence of an Assistant Secretary also mounted. Representative John Dingall (D-MI) concluded that "[t]his noticeable and lengthy absence of cybersecurity leadership conveys a lack of appreciation for our [n]ation's real and mounting cyber threats." [82] Nearly eleven months after the Secretary's announcement, in a June 9, 2006 letter to Secretary Chertoff, Representatives Bennie Thompson (D-MS) and Lofgren noted that the House Committee on Homeland Security[83] had "repeatedly inquired with the Department how it plans to protect vital national cyber interests and how it can do so without steady leadership."[84] The letter

---

[80] Press Release, Cyber Security Industry Alliance, CSIA Renews Call for Stronger Cyber Security Leadership from the Department of Homeland Security (July 12, 2006).

[81] Vijayan, *supra* note 67.

[82] *Id.* (quoting Congressman John Dingell (D-MI)).

[83] In 2002, the U.S. House of Representatives created the Committee on Homeland Security. Initially, the Committee acted as a select, non-permanent Committee, and provided Congressional oversight over the development of the Department of Homeland Security. On January 4, 2005, the first day of the 109th Congress, the House designated the Committed as a Standing Committee, thereby making it a permanent committee. *See, e.g.*, Dep't of Homeland Sec., About the Committee: Homeland Security Committee Overview, http://homeland.house.gov/about/index.asp (also noting that the Committee exercises subpoena power).

[84] Letter from Bennie G. Thompson, Ranking Member, H. Comm. on Homeland Security, and Zoe Lofgren, Ranking Member, H. Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment, to Michael Chertoff, Secretary, Department of Homeland Security (June 9, 2006), *available at* http://hsc.house.gov/press/index.asp?ID=60&SubSection=0&Issue=4&DocumentType=0&PublishDate=2006&issue=4.

continued, "As you know, the Assistant Secretary for Cyber Security Division ("NCSD") is still led by an 'Acting Director."[85] In closing, the Committee asked the Secretary to provide it with answers to several cybersecurity-related questions including "[w]hen will the Department finally name the Assistant Secretary for Cyber Security, which you agreed to create last summer as part of your 'Second Stage Review?"[86]

Clearly frustrated, Representative Thompson asked, "How long will the nation have to wait? I, for one, hope Mr. Chertoff doesn't wait until a cyber attack causes billions of dollars in damages or results in lost lives before he decides to appoint an assistant secretary to take charge of our nation's cyber crisis."[87] On the one-year anniversary of Secretary Chertoff's announcement of the Assistant Secretary position, Representative Thompson publicly criticized the Department.

> [I]t's apparent that the Department is moving at dial-up speed in hardening this infrastructure to respond to cyber attacks. It is hard to take the Department's promises seriously, when, one year later, they still haven't appointed a qualified individual to fill the position of Assistant Secretary for Cyber Security and Telecommunications and have outsourced critical cyber positions within the Department. It boggles the mind that this Administration has not had a top-level cyberczar leading our nation's efforts since 2003.[88]

Lofgren continued to express her disappointment: "At the time [of the announcement], I applauded Chertoff for recognizing the necessity of this position to better protect our nation's cyberinfrastructure from

---

[85] *Id.*

[86] *Id.*

[87] Grant Gross, *Cybersecurity Group Knocks U.S. Government Efforts*, COMPUTERWORLD, Dec. 13, 2005, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=107040&intsrc=article_more_bot.

[88] Press Release, H. Comm. on Homeland Security, Failure to Appoint Leader Leaves Weak Links in Global Cybersecurity Efforts (July 13, 2006), *available at* http://hsc.house.gov/press/index.asp?ID=74&SubSection=1&Issue=4&DocumentType=0&PublishDate=2006&issue=4.

attacks by hackers, criminals and terrorists."[89] But, the prolonged vacancy of the position forced Lofgren to "take back my applause [because] our cyberinfrastructure continues to be at risk."[90] She continued, "On the one-year anniversary of Chertoff's announcement, I am extremely disappointed but unfortunately not surprised that Homeland Security has yet to begin such a critical task . . . . Filling the position of assistant secretary for cybersecurity is the beginning, not the end, of protecting our nation's cyberinfrastructure."[91]

Two months later, the United States General Accountability Office ("GAO") joined the choir of discontent. In September 2006, the GAO released a report titled *DHS Leadership Needed to Enhance Cybersecurity*.[92] The GAO report characterized the limited progress on a variety of Department initiatives and explained that the "relationships among these initiatives were not evident." [93] Consequently, the report noted that the Department was not "adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption."[94] The GAO report concluded that the Department has "many challenges to overcome, several of which will be difficult without effective leadership . . . . Addressing this leadership void starts with DHS naming its Assistant Secretary of Cyber Security and Telecommunications."[95]

F. THE DEPARTMENT'S BIG ANNOUNCEMENT (ROUND 2)

Finally, the Department acted. On September 18, 2006, more than fourteen months since the Department first established the position, Secretary Chertoff announced the appointment of Greg Garcia as

---

[89] Zoe Lofgren, *Rescinding my Applause for Chertoff*, CNET NEWS, July 14, 2006, http://www.news.com/rescinding-my-applause-for-Chertoff/2010-1028_3-6093654.html.

[90] *Id.*

[91] *Id.*

[92] U.S. GEN. ACCOUNTABILITY OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: DHS LEADERSHIP NEEDED TO ENHANCE CYBERSECURITY 1 (2006), http://www.gao.gov/new.items/d061087t.pdf.

[93] *Id.* at 9.

[94] *Id.*

[95] *Id.* at 17.

Assistant Secretary for Cyber Security and Telecommunications.[96] According to Secretary Chertoff, Garcia possessed the right mix of "experience in government and the private sector to continue to strengthen our robust partnerships that are essential to this field. He has the expertise to focus resources and activities within the cyber and telecommunications communities in a manner that is consistent with our risk-based approach to homeland security."[97] Shannon Kellogg, director of government and industry affairs at RSA, the security division of the EMC Corporation, seemed pleased with Garcia's appointment. "He's a solid choice and will do a good job."[98] But Kellogg cautioned, "At the same time, it's important for him not to go in there and try to boil the ocean. He needs to choose three or four key priorities on cyber and work to move those forward."[99]

Once the Department had an Assistant Secretary of Cybersecurity in place, the pressure to perform was enormous. Garcia received mixed reviews after he took the helm as Assistant Secretary. When asked about Garcia's performance to date, former NCSD director Amit Yoran answered, "There is so much that is on Assistant Secretary Garcia's plate that is critical, and the ability to respond [to cyber attacks] is so difficult to measure."[100] Yoran believes that Garcia has succeeded in expanding the awareness of cyber threats and the need for better security. "Is progress being made? I would say yes. Is it sufficient? That's harder to say . . . there's certainly a lot more that still needs to be done."[101] According to Yoran, "Garcia is doing certain

---

[96] Press Release, Dep't of Homeland Sec., Statement by Homeland Security Secretary Michael Chertoff on the Appointment of the Assistant Secretary for Cyber Security Telecommunications (Sept. 18, 2006), *available at* http://www.dhs.gov/xnews/releases/pr_1158759756150.shtm.

[97] *Id.*

[98] Brian Krebs, *Top Cyber-Security Post Is Filled*, WASH. POST, Sept. 18, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/09/18/AR2006091800928.html.

[99] *Id.*

[100] Brian Robinson, *Gregory Garcia: His First Year as Cybersecurity Czar*, FED. COMPUTER WK., Nov. 12, 2007, http://www.fcw.com/print/13_40/features/150748-1.html.

[101] *Id.*

things very well, but there's still a lot that isn't fully understood. I can't say whether overall he's doing an A or a C level job."[102]

Others in the industry are more optimistic. Jim Lewis, the director the Center for Strategic and International Studies' technology and public policy program, stated that "[t]here's no doubt [Garcia's] won the beauty contest vote, and most people seem to think he's done a good job. But, [it is] too early to rate how the DHS overall is doing on cybersecurity."[103] Shannon Kellogg[104] commended Garcia for his pragmatic approach, and noted that Garcia did not attempt to "boil the ocean, but rather, Garcia identified three or four priorities and continued to stress those priorities."[105] Garcia's priorities included an effort to bring into harmony the Department's various components, and to improve the process for sharing information between the government and industry.[106] Others believe that Garcia's success is attributable, in part, to his credibility in the industry. Liesyl Franz, Vice-President of Information Security Programs and Policy at the Information Technology Association of America, believes that Garcia's background strengthened his credibility. Franz noted:

> Industry called for the [assistant secretary] position and also called for the person appointed to be from the private sector, because there is a big role that the private sector needs to play in incidence response. With regard to that, Garcia and his staff have been exemplary in building coordination between the various parties.[107]

Nevertheless, what appeared to be a successful first year for Garcia as the Assistant Secretary did not alleviate Congressional concerns regarding the Department's cyber security leadership and leadership

---

[102] *Id.*

[103] *Id.*

[104] Kellogg was the Director of Information Security Policy, Office of Government Relations at EMC Corporation.

[105] Robinson, *supra* note 100.

[106] *Id.*

[107] *Id.*

in general. In July 2007, Representative Thompson described the effects of the ongoing leadership crisis.

> [W]hat's worse than a Homeland Security organization with poor leadership is a homeland security organization with no leadership. Not just a national security concern, DHS's lack of leadership has triggered record-low employee morale, an immeasurable disservice to the hundreds of thousands of men and women working on the front lines to protect our country.[108]

Thompson's tirade referenced a July 2006 survey released by the Office of Personnel Management ("OPM"). The OPM conducted a survey of thirty-six federal offices and agencies,[109] and the survey demonstrated that the Department ranked last or near to last in every category. [110] For example, the Department ranked last in job satisfaction[111] and results-oriented performance, and next to last on leadership.[112]

---

[108] Press Release, Vacancy Report Finds Homeland Security and Continuity of Government at Risk (July 9, 2007), *available at* http://hsc.house.gov/press/index.asp?ID=237&SubSection=0&Issue=0&DocumentType=0&PublishDate=0.

[109] *See* Stephen Losey, *DHS Leaders Aim to Turn Around Poor Morale*, FED. TIMES, Sept. 18, 2007, http://www.federaltimes.com/index.php?S=3047128.

[110] *Homeland Security Employees Rank Last in Job Satisfaction Survey*, ABC NEWS, Feb. 8, 2007, http://abclocal.go.com/wls/story?section=nation_world&id=5017688; *see also* http://www.fhcs.opm.gov/2006FILES/FHCS_2006_AgencyReport_Part5.pdf. On February 8, 2007, the President made his first visit in three-and-a-half years to the Homeland Security headquarters, a place that internal employees describe as the worst place in the federal government to work.

[111] For example, the survey noted that only 57% of Department employees reported satisfaction with their jobs. This figure was about 10% less than the government wide job satisfaction rate of 67.5%. *See* Losey, *supra* note 109.

[112] *Homeland Security Employees Rank Last in Job Satisfaction Survey, supra* note 110; *see also* http://www.fhcs2006.opm.gov/Published/FHCS_2006_AgencyReport_Part5.pdf.

III. WHO OR WHAT JEOPARDIZE AMERICAN CYBER SECURITY?

According to Richard Clarke, the former Chair of the President's Critical Infrastructure Protection Board, the threat to cyberspace is "really very easy to understand. If there are major vulnerabilities in the digital networks that make our country run, then someday, somebody will exploit them in a major way doing great damage to the economy." [113] Clarke explained that the exploitation of such vulnerabilities will likely be devastating. "Transportation systems could grind to a halt. Electric power and natural gas systems could malfunction. Manufacturing could freeze. 911 emergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled . . . our forces [will be] at great risk by having their logistics system fail."[114] The potential for panic among the American people is real, and it is frightening. Accordingly, this article explores the persistent threats to the nation's cyber security and the Department's efforts to combat those threats, and concludes that the current organizational infrastructure of the Department is ill-conceived and ill-equipped to secure the nation's cyber infrastructure.

A. ONE MAN'S CRUSADE AGAINST TITAN RAIN

In September 2003, security analyst Shawn Carpenter, an employee at Sandia National Laboratories ("Sandia"), [115] helped to investigate a network break-in at Lockheed Martin.[116] A few months later, Sandia's systems experienced a similar attack. [117] After consulting with a counterpart in the Army's cyber intelligence unit, Carpenter identified a relationship between what appeared to be two independent cyber attacks.[118] That realization prompted Carpenter to

---

[113] *Major Cyberspace Vulnerabilities, supra* note 17.

[114] *Id.*

[115] Sandia National Laboratories, About, http://www.sandia.gov/about/index.html (last visited Feb. 12, 2009).

[116] Nathan Thornburgh, *The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)*, TIME, Aug. 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098906,00.html.

[117] *Id.*

[118] Thornburgh, *supra* note 116.

initiate an unofficial investigation of these attacks. Since the Army had experienced several similar attacks, Carpenter told his Sandia superiors that he intended to share with the Army any findings that the investigation might yield.[119]

For the better portion of the next year, Carpenter continued his investigation. In March 2004, Carpenter—who the FBI later dubbed 'Spiderman'—first discovered the activities of these cyber hackers.[120] Carpenter had pursued a group of suspected Chinese cyber hackers as the group deftly navigated the cyber world. The cyber hackers executed an unrelenting series of coordinated attacks that are now collectively referred to as TITAN RAIN.[121] As promised, Carpenter shared his findings with several unofficial Army contacts.[122] By October 2004, Carpenter's Army contacts had introduced Carpenter to the FBI, and the FBI learned the nature of Carpenter's investigation.[123] Carpenter claimed that, for the next five months, he served as a confidential informant for the FBI.[124] Carpenter's work soon reached the most senior levels of the FBI's counterintelligence division, where the FBI allegedly incorporated Carpenter's work into an existing task force.[125]

As Carpenter explored the activities of TITAN RAIN, he noted that the cyber hackers worked very, very quickly and with a definite sense of purpose.[126] The sophistication of the attacks and the attackers captivated Carpenter. "Most hackers, if they actually get into a government network, get excited and make mistakes. Not these guys. They never hit a wrong key."[127] According to Carpenter, the hackers would commandeer hidden sections of hard drives, consolidate as many files as possible, and immediately transmit the files to work

---

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] Thornburgh, *supra* note 116.

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] *Id.*

stations in South Korea, Hong Kong, or Taiwan.[128] From these locations, the cyber hackers sent the files to mainland China.[129] Carpenter pursued these cyber hackers until the trail ended in the southern Chinese province of Guandong.[130] The TITAN RAIN attacks emanated from just three Chinese routers.[131] When Carpenter uncovered the TITAN RAIN routers, he carefully installed into the primary router's software a homemade bugging code.[132] Carpenter designed the bugging code to send an e-mail alert to an anonymous Yahoo! e-mail account each time the cyber hackers made a move on the Internet.[133] Within two weeks the software delivered over 23,000 messages to Carpenter's anonymous e-mail account.[134]

Carpenter's work led to some startling discoveries. In late May 2004, Carpenter uncovered a cache of stolen documents that the cyber hackers had stored in zombie servers in South Korea.[135] In addition to American military information, Carpenter uncovered hundreds of documents concerning the detailed schematics of propulsion systems, solar paneling, and fuel tanks for the Mars Reconnaissance Orbiter.[136] Carpenter also copied an enormous collection of files that the cyber hackers had stolen from Redstone Arsenal, which is home to the Army Aviation and Missile Command.[137] These files included the specifications for aviation mission planning systems for Army helicopters.[138]

As Carpenter shared with the FBI the information that he had gathered, the agents assigned to Carpenter assured him that the work

---

[128] Thornburgh, *supra* note 116.

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] Thornburgh, *supra* note 116.

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] Thornburgh, *supra* note 116.

was justified. [139] When the FBI asked Carpenter to stop the investigation so that the agents could obtain additional authorization, Carpenter continued to provide the FBI with additional analysis of the information that he initially collected.[140] According to Carpenter, FBI agent Christine Pas praised Carpenter for his contributions,[141] noting that Carpenter's work "could very well impact national security at the highest levels."[142] In March 2005, after months of correspondence, the FBI suddenly ceased to communicate with Carpenter; an action which surprised Carpenter.[143] A source in federal law enforcement told TIME Magazine that while the FBI was working with Carpenter, the agency was simultaneously investigating Carpenter and his cyber activities.[144]

Despite the apparent value of Carpenter's work, Sandia did not welcome news of Carpenter's after-hour cyber activities. Carpenter explained that after the FBI contacted Sandia to discuss the extent of Carpenter's activities, Sandia fired Carpenter and stripped him of his Q security clearance.[145] Ultimately, the United States Attorney elected not to press charges against Carpenter. Because Carpenter believed that the military, FBI, and to some extent, Sandia, unofficially encouraged him to continue his work, Carpenter felt betrayed by their respective actions. Consequently, in August 2005, Carpenter filed in New Mexico State court a lawsuit against Sandia for defamation and wrongful termination. Subsequently, the jury awarded Carpenter $4.3 million in punitive damages, $350,000 for emotional distress, and more than $36,000 for lost wages, benefits, and other costs.[146]

---

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] Thornburgh, *supra* note 116.

[145] *Id.*

[146] Jaikumar Vijayan, *Reverse Hacker Wins $4.3M in Suit Against Sandia Labs*, COMPUTERWORLD, Feb. 14, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=standards_and_legal_issues&articleId=9011283.

C. THE PROOF IS IN THE PUDDING

Carpenter's description of the cyber hackers' proficiency and sense of purpose is not an exaggeration. Consider this series of coordinated attacks on American interests. On November 11, 2004, at 10:23 PM Pacific Standard Time ("PST"), Chinese hackers detected a vulnerability at the United States Army Information Systems Engineering Command at Fort Huachuca, Arizona.[147] At 1:19AM PST, hackers then attacked the same vulnerability in computers at the military's Defense Information Systems Agency in Arlington, Virginia.[148] Again, at 3:25 AM PST, the hackers hit the Naval Ocean Systems Center, a defense department installation in San Diego, California.[149] And again, at 4:46 AM PST, the hackers penetrated the Army's Space and Strategic Defense Installation in Huntsville, Alabama.[150] Regarding these attacks, Allen Paller, director of the SANS Institute, stated:

> The precision of the attacks, the perfection of the methods and the 24-by-seven operations over two and a half years, and the number of workstations involved are simply not replicated in the amateur criminal community . . . . [T]his is an order of magnitude more disciplined than anything I have seen out of the hacker or amateur criminal community.[151]

Paller noted that "[t]hese attacks come from someone with intense discipline . . . . [These hackers] were in and out with no keystroke errors and left no fingerprints, and created a backdoor in less than

---

[147] Nathan Thornburgh, *Inside the Chinese Hack Attack*, TIME, Aug. 25, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html.

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] Larry Greenemeier, *China's Cyber Attacks Signal New Battlefield Is Online*, SCIENTIFIC AMER., Sept. 18, 2007, http://www.sciam.com/article.cfm?articleID=1A9C210F-E7F2-99DF-3C85F17B1680980D&sc=I100322 (statement of Alan Paller, Director of Research at the SANS ("SysAdmin, Audit, Network, Security") Institute, which trains and certifies technology workers in cyber security).

thirty minutes. How can this be done by anyone other than a military organization?"[152]

More recently, in June 2007, cyber hackers attacked the computer networks servicing the Pentagon. The Pentagon acknowledged that this particular cyber attack forced officials to shut down computers that served the office of Defense Secretary Robert Gates.[153] Although the Pentagon did not confirm the exact number of affected computers, estimates placed the number around 1,500.[154] Regarding the attacks, Secretary Gates stated, "Elements of the OSD unclassified e-mail system were taken offline yesterday afternoon, due to a detected penetration."[155] Characterized as the most successful cyber attack to date on the United States Defense Department,[156] a person familiar with the attack said the officials believe with a "very high level of confidence . . . trending towards total certainty" that the People's Liberation Army of China ("PLA") perpetrated the June 2007 attack.[157]

Gates also offered this sobering comment: "The reality is that the Defense Department is constantly under attack . . . hundreds of attacks" per day.[158] For example, in 2005, the Pentagon recorded more than 79,000 attempted intrusions. Approximately 1,300 of such attempts were successful, including the penetration of systems linked to the Army's 82nd and 101st Airborne Divisions and the 4th Infantry Division.[159] Furthermore, more attempts to scan the systems that

---

[152] *Hacker Attacks in US Linked to Chinese Military: Researchers*, BREITBART.COM, Dec. 12, 2005, http://lists.jammed.com/ISN/2005/12/0059.html.

[153] Katherine Noyes, *Pentagon Shrugs Off Cyber-Attack*, TECH NEWS WORLD, June 22, 2007, http://www.technewsworld.com/story/57990.html.

[154] *Id.*

[155] Interview with Robert M. Gates, Sec. of Defense & Peter Pace, Joint Chiefs of Staff Gen., Arlington, Va. (June 21, 2007), *available at* http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[156] Demetri Sevastopulo & Richard McGregor, *Chinese Military Hacked into Pentagon*, FINANCIAL TIMES, Sept. 3, 2007, http://search.ft.com/ftArticle?queryText=chinese+hacked&aje=true&id=070903008457&ct=0.

[157] *Id.*

[158] Noyes, *supra* note 153.

[159] Tim Reid, *China's Cyber Army is Preparing to March on America, Says Pentagon*, TIMES ONLINE, Sept. 8, 2007,

serve the Defense Department originate in China than in any other country in the world.[160]

Alex Neill, the head of the Asia Security Programme at the Royal United Services Institute, described the June 2007 attack on the Pentagon as the "most flagrant and brazen to date."[161] Neill characterized this attack as "pressure point warfare[;]" a new PLA strategy comprising the identification and attack of specific targets that will paralyze the adversary.[162] Specifically, China is integrating into its military operations "information warfare units" that have the capability for "first strikes against enemy networks."[163] Peter W. Rodman, the United States Assistant Secretary of Defense for International Security Affairs, summarized the current situation:

> We all know how great the Chinese people are at information technology. And the People's Liberation Army is tapping into some of that expertise to make significant strides in cyber warfare and China is exploring not only defensive activities defending its computer networks from attack but is also exploring offensive operations against an adversary's computer networks.[164]

Richard Lawless, the Pentagon's top Asia official at the time of the June 2007 attack, likened these cyber attacks to "multiple wake-up

---

http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece.

[160] Bradley Graham, *Hackers Attack Via Chinese Web Sites*, WASH. POST, Aug. 25, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318_pf.html.

[161] Richard Norton-Taylor, *Titan Rain - How Chinese Hackers Targeted Whitehall*, THE GUARDIAN, Sept. 5, 2007, http://www.guardian.co.uk/technology/2007/sep/04/news.internet.

[162] *Id.*

[163] DEPT. OF DEFENSE, ANNUAL REPORT TO CONGRESS: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 35–36 (2006), *available at* http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf.

[164] Peter W. Rodman, U.S. Assistant Secretary of Defense for International Security Affairs, Keynote Address at the Chicago Society Symposium: China and the Future of the World (Apr. 29, 2006), *available at* http://chicagosociety.uchicago.edu/china/coverage/RodmanSpeech.pdf.

calls stirring us to levels of more aggressive vigilance."[165] He noted that although the PLA regularly probes American military networks, the penetration in June raised concerns to a new level because the Pentagon attack demonstrated that China could disrupt important military systems at a critical time.[166]

IV. THE MOUNTING TENSION BETWEEN CONGREE AND THE DEPARTMENT

Since its inception, the Department's relationship with Congress has, at best, been strained. In 2002, the U.S. House of Representatives created the Committee on Homeland Security. The House of Representatives charged the Committee with the task of providing Congressional oversight for the Department's development. On January 4, 2005, the first day of the 109th Congress, Congress made the Committee a permanent standing committee. [167] The Committee then adopted a set of operating rules.[168]

Congress recognized that the Department's hierarchy created problems with the nation's cybersecurity leadership. Following the series of resignations that included Yoran Amit and Robert Liscouski, Representative Zoe Lofgren (D-CA) concluded, "Quite simply, our nation has been without adequate leadership on cybersecurity since Howard Schmidt resigned the cybersecurity czar position in 2003."[169] According to Lofgren, the Nation's top cybersecurity position was now "a 'directorship' buried within the bureaucracy of Homeland Security."[170] She explained that since Yoran's resignation, "Homeland Security has contracted out the position to an acting director who is being paid $577,000 under a two-year contract. That is almost a

---

[165] Sevastopulo & McGregor, *supra* note 156.

[166] *Id.*

[167] United States H.R. Comm. on Homeland Sec., About the Committee, http://hsc.house.gov/about/index.asp (last visited Apr. 15, 2009).

[168] United States H.R.Comm. on Homeland Sec., Committee Rules, http://hsc.house.gov/documents/chsrules110th.pdf (last visited Apr. 15, 2009).

[169] Zoe Lofgren, *Rescinding my Applause for Chertoff*, CNET NEWS, July 13, 2006, http://www.news.com/rescinding-my-applause-for-Chertoff/2010-1028_3-6093654.html. *See also* discussion, *supra* notes 47–65.

[170] *Id.*

quarter million more than Chertoff is being paid as the top official at the department. Meanwhile, cyberspace remains vulnerable."[171] On September 14, 2004, Representatives Lofgren and Mac Thornberry (R-TX) introduced into the House of Representatives H.R. 5068, titled the *Department of Homeland Cybersecurity Enhancement Act of 2004*. Section 203 of H.R. 5068 read: "There shall be in the Directorate for Information Analysis and Infrastructure Protection a National Cybersecurity Office headed by an Assistant Secretary for Cybersecurity . . . who shall assist the Secretary in promoting cybersecurity for the Nation."[172] On September 24, 2004, the House of Representative referred H.R. 5068 to the House Subcommittee on Cybersecurity, Science, and Research and Development;[173] however, the end of the congressional term prevented any further action regarding the bill.[174] When, in January 2005, the 109th Congress took office, Representatives Lofgren and Thornberry re-introduced into the House the bill as H.R. 285.[175]

A. THE HOUSE COMMITTEE ON HOMELAND SECURITY DEMANDS ANSWERS

To assess the Department's awareness and responsiveness to emerging cyber threats, on April 30, 2007, the House Committee on Homeland Security mailed to Scott Charbo, the Department's Chief Information Officer ("CIO") a letter requesting the answers to several probing questions.[176] When the Committee learned that, during fiscal

---

[171] *Id.*

[172] Department of Homeland Security Cybersecurity Enhancement Act of 2004, H.R. 5068, 108th Cong. § 203 (2004), *available at* http://www.govtrack.us/data/us/bills.text/108/h/h5068.pdf.

[173] *See* The Library of Congress: Thomas, H.R. 5068, http://www.thomas.gov/cgi-bin/bdquery/z?d108:h.r.05068:.

[174] *See id.*

[175] Department of Homeland Security Cybersecurity Enhancement Act of 2005, H.R. 285, 109th Cong. (2005), *available at* http://www.thomas.gov/cgi-bin/bdquery/z?d109:h.r.00285:.

[176] Letter from Bennie G. Thompson, Chairman, H. Comm. on Homeland Security, James R. Langevin, Chairman, H. Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology, to Scott Charbo, Chief Information Officer, Department of Homeland Security (Apr. 30, 2007), *available at* http://homeland.house.gov/SiteDocuments/Charbo.pdf.

years 2005 and 2006, the Department networks experienced 844 "cybersecurity incidents,"[177] Representative Langevin responded, "[i]t was a shock and a disappointment to learn that the Department of Homeland Security—the agency charged with being the *lead* in our national cybersecurity—has suffered so many significant security incidents on its networks."[178] But, others in the industry believe that the number of incidents is much higher. For example, Allen Paller said that the "reality is that the federal agencies don't report all of them. Eight hundred and forty-four is a big number, but it's a sample of the reality, not the total reality."[179] Paller cautioned, "You don't know about all of them. That I can guarantee. And in particular, you're not knowing about the worst ones."[180] Paller explained that in cases of "really embarrassing event[s]," many agencies believe that "it's less of a problem to not tell, than to tell and be beaten up about it."[181]

As the congressional investigation continued, the Committee noted that there was an uncanny similarity between the attacks on the network systems servicing the Department's systems and recent attacks on the network systems of the Commerce Department.[182] Specifically, the Committee noticed recurring patterns of infection

---

[177] *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security: Hearing Before the H. Comm. on Homeland Security*, 110th Cong. (2007) (statement of James R. Langevin, Chairman, H. Subcomm. on Homeland Security Emerging Threats, Cyberscurity, and Science and Technology), *available at* http://homeland.house.gov/SiteDocuments/20070620144327-44568.pdf. The affected networks serviced the Department headquarters as well as networks servicing Immigration and Customs Enforcement and Federal Emergency Management Agency.

[178] *Id.*

[179] Sharon Gaudin, *Feds' Own Hacker Cracks Homeland Security Network*, INFO.WK., June 21, 2007, http://www.informationweek.com/news/showArticle.jhtml;jsessionid=QP2ZKN2L25KZYQSNDLRSKHoCJUNN2JVN?articleID=199906038&pgno=1&queryText=.

[180] *Id.*

[181] *Id.*

[182] Letter from Bennie G. Thompson, Chairman, H. Comm. on Homeland Security, and James R. Langevin, Chairman, H. Subcomm. of Emerging Threats, Cybersecurity, and Science and Technology, to Richard L. Skinner, Inspector General, Department of Homeland Security (Sept. 21, 2007), *available at* http://hsc.house.gov/SiteDocuments/20070924104629-96412.pdf.

that included password dumping utilities and other Trojan horse activity with suspicious beaconing activity.[183] This beaconing activity suggests the placement inside a computer of malicious code, which is attempting to communicate with an outside entity.[184] Consequently, the Committee concluded that the "Department is the victim not only of cyber attacks initiated by foreign entities, but of incompetent and possibly illegal activity by the contractor charged with maintaining security on its networks."[185]

During a private conversation, and again at a June 20, 2007 hearing, titled *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security*, Representative Langevin asked Charbo two questions.[186] First, whether Charbo and his security team requested or received intelligence briefings regarding the penetration of federal networks by Chinese hackers. Second, whether the Department computers exfiltrated information to Chinese servers. Charbo's response, which included the statement "you don't know what you don't know," suggested to the Committee that "neither he nor the rest of the Department was taking this issue seriously . . . ."[187] Langevin concluded:

> The fact is, DHS is failing to dedicate adequate funding to network security. The finances show that Mr. Charbo and the Department's leadership continue to underinvest in IT security. Mr. Charbo cut funding for the Chief Information Security Officer and only slightly increased the IT security budget. Experts agree that agencies should allocate around 20% of their IT budgets to cybersecurity, and yet DHS is only spending 6.8% to secure their systems. And all of this is

---

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

> happening while the Department's IT budget was increased by $1 billion last year.[188]

In an attempt to defend the Department, Charbo explained that by the end of the year 2007, the Department will have spent $4.9 billion for information technology, including $332 million for IT security.[189] Charbo also noted that the Department planned to ask for $5.2 billion for the year 2008, including $342 million or 6.8% for security.[190] Unsatisfied by Charbo's response, Representative Langevin concluded that Department's leadership continued to under-invest in information technology.[191]

Representative Thompson also expressed his outrage, and explained that the Department's "'[d]o as I say, not as I do' policy is a recipe for disaster." Thompson warned that if the Department was serious about cyber risks, then it "need[ed] to start acting and stop posturing."[192]

> How can the Department of Homeland Security be a real advocate for sound cybersecurity practices without following some of its own advice? How can we expect improvements in private infrastructure cyberdefense when DHS bureaucrats aren't fixing their own configurations? How can we ask others to invest in upgraded security technologies when the Chief Information Officer grows the Department's IT security budget at a snail's pace? How can we ask the private

---

[188] *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security*, *supra* note 177.

[189] *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security: Hearing Before the H. Comm. on Homeland Security*, 110th Cong. (2007) (statement of Scott Charbo, Chief Information Office, Department of Homeland Security), *available at* http://homeland.house.gov/SiteDocuments/20070620144403-36627.pdf.

[190] *Id.*

[191] *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security*, *supra* note 177.

[192] *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security: Hearing Before the H. Comm. on Homeland Security*, 110th Cong. (2007) (statement of Bennie G. Thompson, Chairman, H. Comm. on Homeland Security), *available at* http://homeland.house.gov/SiteDocuments/20070620144350-15564.pdf.

> sector to better train employees and implement more consistent access controls when DHS allows employees to send classified emails over unclassified networks and contractors to attach unapproved laptops to the network?[193]

Thompson explained that Charbo did not "convince [him] that he's serious about fixing the vulnerabilities in our systems."[194] Quoting Ralph Waldo Emerson, Thompson told Charbo and the Department, "What you do speaks so loud that I cannot hear what you say."[195]

B. THE GOVERNMENT HACKS THE DEPARTMENT

As the federal government's top hacker, Keith A. Rhodes has a congressional mandate to test the network security of twenty-four different federal agencies and departments.[196] Each year, Rhodes, the GAO's Chief Technologist and Director of its Center for Technology and Engineering, performs ten penetration tests on these agencies and departments. For approximately one year, Rhodes tested the Department's network.[197] During a congressional hearing, Rhodes discussed the disturbing results of his investigation. When asked about the cybersecurity of the U.S. Visit program, Rhodes responded:

> Security issues are pervasive. As matter of fact, I realize that there was an earlier statement that our audit was a year old, but actually our audit started a year ago. As matter of fact, we curtailed our assessment since we kept getting more and more findings. If we continued to this day, we would still be finding problems. The problems are pervasive and systemic. Actually, a lot could be fixed. Systems were out of date or misconfigured. A lot of them are zero

---

[193] *Id.*

[194] *Id.*

[195] *Id.*

[196] Gaudin, *supra* note 179.

[197] *Id.*

> cost fixes. I reiterate the systems are run by contractors.[198]

Lofgren then asked, "Was the U.S. Visit database hacked?" Rhodes explained that he "did not see controls in place that would prevent [an intrusion] and did not see defensive perimeter and detection systems in place to tell whether it had or had not been hacked."[199]

Rhodes further noted that certain Department systems were "riddled with significant information security control weaknesses that placed sensitive and personally identifiable information at increased risk of unauthorized disclosure and modification, misuse, and destruction possibly without detection, and place program operations at increased risk of disruption."[200] He further admitted that "[t]o understand how the system was set up and what it was doing, we had to talk to contractors."[201]

In a post-hearing interview, Rhodes offered that he "would label [the Department] as being at high risk. There was no system we tested that didn't have problems. There was nothing we touched that didn't have weaknesses . . . ."[202] Finally, Rhodes admitted that "[i]f we had continued the audit we would have found more . . . we just ran out of room in our basket."[203] The implications of this testimony are unsettling. Representative Langevin summarized Rhodes compelling testimony as follows:

> What does this mean? It means that terrorists or nation states could be hacking Department of Homeland Security databases, changing or altering their names to allow them access to this country, and we wouldn't even know that they were doing it. If we

---

[198] Ryan Singel, *Lofgren Asks if US VISIT Hacked; Wired Has Proof Answer is Yes*, WIRED, June 20, 2007, http://blog.wired.com/27bstroke6/2007/06/lofgren_asks_if.html.

[199] *Id.*

[200] U.S. GEN. ACCOUNTABILITY OFFICE, INFORMATION SECURITY: HOMELAND SECURITY NEEDS TO ENHANCE EFFECTIVENESS OF ITS PROGRAM 10 (2007), http://homeland.house.gov/SiteDocuments/20070620144440-80444.pdf.

[201] Gaudin, *supra* note 179.

[202] *Id.*

[203] *Id.*

> care about protecting our homeland from dangerous people, we have to care about the security of the information that we use to accomplish that missions.[204]

C. THE COMMITTEE GETS THE DEPARTMENT'S INSPECTOR GENERAL INVOLVED

The Committee's investigation continued with a September 21, 2007 letter to Richard L. Skinner, the Department's Inspector General ("IG").[205] In the letter, the Committee detailed a series of cyber incidents that occurred at the Department, which included the "placement of a hacking tool, a password dumping utility, and other malicious code on over a dozen computers."[206] Furthermore, despite the fact that hackers exfiltrated information from the Department's systems to a web hosting system that connected to Chinese websites, the Department did not notice these intrusions for months after the attacks transpired.[207] Government contractors provided to the Department inaccurate and misleading information regarding the source of the cyber attacks, and attempted to hide gaps in their security capabilities.[208] Lastly, when the Department finally recognized the extent of these cyber attacks, the Department preferred to complete the fiscal year's financial transactions rather than take immediate steps to mitigate the problems.[209]

Before ending the letter, the Committee reminded the Inspector General that, "as you know, 18 U.S.C. § 1001 makes it a crime to knowingly and willingly make a materially false, fictitious or fraudulent statement or representation to the United States government."[210] In short, if the Department determined that violations of federal law had occurred, then the Committee expected

---

[204] *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security*, *supra* note 177.

[205] Letter from Thompson & Langevin, *supra* note 182.

[206] *Id.*

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] *Id.*

the Department to report to the Justice Department those violations and the offending parties.[211] Finally, the Committee lamented, "[W]e are disappointed by the Department's misleading responses to the Committee's requests for information, and request that you determine whether the intent of these misstatements was to obstruct the Committee's investigation."[212]

D. THE COMMITTEE ADVISES THE DEPARTMENT NOT TO GO IT ALONE

On October 22, 2007, Representative Thompson sent Secretary Chertoff a letter demanding information regarding certain Department activities "that—if undertaken—will have a major impact on the cybersecurity posture of the United States."[213] Specifically, Thompson noted that on September 22, 2007, the *Baltimore Sun* discussed an interagency cyber initiation between the National Security Agency and the Department.[214] Thompson's frustration with the Department's lack of communication was obvious. Thompson wrote, "On at least four separate occasions, my staff has tried to schedule briefings from the department on this effort. Each time, the department refused to do so."[215] At an October 17, 2007 hearing, Thompson asked Assistant Secretary Greg Garcia to provide the Committee with information regarding this initiative, but "[a]gain, my request was met with silence . . . . I certainly hope that the Department does not plan to go forward with this program without fully briefing this Committee . . . ."[216]

The Department's spokesperson, Laura Keehner, refuted Thompson's allegation. Keehner noted that, in the past year, the Department met with the Committee more than six times to discuss cybersecurity and related issues.[217] "We have continually kept

---

[211] *Id.*

[212] *Id.*

[213] Letter from Bennie G. Thompson, Chairman, H. Comm. on Homeland Security, to Michael Chertoff, Secretary, Department of Homeland Security (Oct. 22, 2007), *available at* http://hsc.house.gov/SiteDocuments/20071024093549-09517.pdf.

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] Jason Miller, *Rep. Thompson Presses DHS for Information on Cyber Initiative*, FED. COMPUTER WK., Oct. 24, 2007, http://www.fcw.com/online/news/150595-1.html.

members of Congress involved and will continue to do so. We will respond to his letter in a timely fashion."[218]

More recently, the Senate Committee on Homeland Security and Governmental Affairs locked horns over the Comprehensive National Security Initiative ("CNCI"). On January 8, 2008, President Bush approved National Security Presidential Directive 54 (also Homeland Security Presidential Directive 23). The Directive formalized a multi-agency, multi-year plan that establishes twelve steps to securing the government's cyber networks.[219] On March 20, 2008, Secretary Chertoff announced the appointment of Rod Beckstrom as the first Director of the National Cyber Security Center ("NCSC").[220] According to the Department, the NCSC "will bring together federal cybersecurity organizations, by virtually connecting and in some cases, physically collocating personnel and resources to gain a clearer understanding of the overall cybersecurity picture of Federal networks."[221] Chertoff explained that Beckstrom's tasks included "coordinating cybersecurity efforts and improving situational awareness and information sharing across the federal government."[222] As a co-author of *The Starfish and the Spider: The Unstoppable Power of Leaderless Organization*,[223] a book that discusses the power of decentralized networks in organizations and presents a new model

---

[218] *Id.*

[219] *See* Dep't of Homeland Sec., Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks, April 8, 2008, http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm; *see also* Letter from Joseph I. Lieberman, Chairman, S. Comm. on Homeland Security and Governmental Affairs, to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=a32aba11-4443-4577-b9a5-3b2ea2c2f826&Affiliation=C.

[220] Press Release, Department of Homeland Security, Statement by Homeland Security Secretary Michael Chertoff on the Appointment of the Director of the National Cyber Security Center (March 20, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1206047924712.shtm.

[221] *See* Dep't of Homeland Sec., Fact Sheet, *supra* note 219.

[222] Homeland Security Press Release, *supra* note 220. According to Chertoff, "Rod has over 25 years of experience in designing and implementing new Internet technologies. He brings to the department a specialized Internet expertise, and unique entrepreneurial and creative business thinking." *Id.*

[223] ORI BRAFMAN & ROD A. BECKSTROM. THE STARFISH AND THE SPIDER: THE UNSTOPPABLE POWER OF LEADERLESS ORGANIZATIONS (2008).

for analyzing organizations, leadership style and competitive strategy, Beckstrom's appointment was promising.[224]

Nevertheless, the Senate Committee chastised the Department for its failure to be more forthcoming with respect to the CNCI. For example, the Senate Committee explained that the Department had publicly revealed information that had been previously presented to Senate Committee staff as classified. Furthermore, prior to Chertoff's March 20, 2008 appointment of Beckstrom as the Director of the NCSC, Senate Committee staff had been instructed that the existence of the NCSC itself was classified. Thus, the Senate Committee provided the Department with a series of questions regarding the NCSC, contracting, classification, role of the public, metrics, private sector, privacy impact assessments, and other responsibilities of the Department.[225]

E. THE ACCUSATIONS OF OBSTRUCTION

Some have wondered whether the Department obstructed investigations regarding its activities. In February 2007, David Walker, the Comptroller General of the United States, testified at a hearing titled *An Overview of Issues and Challenges Facing the Department of Homeland Security*. Walker explained:

> DHS has not made its management or operational decisions transparent enough so that Congress can be sure it is effectively, efficiently, and economically using the billions of dollars in funding it receives annually . . . . Our work . . . has been significantly hampered by long delays in granting us access to

---

[224] Less than one year after his appointment, Beckstrom resigned as Director of NSNC. *See* Jaikumar Vijayan, *Federal Cybersecurity Director Quits, Complains of NSA Role*, COMPUTERWORLD, Mar. 8, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9129218. The Wall Street Journal published Beckstrom's resignation letter, *available at* http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf.

[225] Press Release, Senate Committee on Homeland Security and Governmental Affairs, Lieberman and Collins Step Up Scrutiny of Cyber Security Initiative: Secrecy, Overuse of Contractors, Role of Private Sector at Stake (May 2, 2008), *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=a32aba11-4443-4577-b9a5-3b2ea2c2f826&Affiliation=C.

> program documents and officials, or by questioning our access to information needed to conduct our reviews.[226]

Walker continued, "While much of its sensitive work needs to be guarded from improper disclosure, DHS has not been receptive towards oversight and its delays in providing Congress and us with access to various documents and officials have impeded our work."[227] He lamented, "When you have more lawyers in a meeting than program people, you know you got a problem. Something needs to be done about this."[228] Walker suggested that the involvement of the Department's General Counsel in such investigatory proceedings should be an exception rather than the rule.[229] "Right now the system is structured to delay, delay, delay . . . . We haven't had a situation where they refuse information but it might take months to get it."[230] Because all requests had to go through the General Counsel's office, Walker also faced "systemic" and "persistent" problems trying to obtain documents from the Department. [231] Following Walker's testimony, Representative David Price (D-NC), offered this sentiment of comfort: "You can be assured that we hear you loud and clear."[232] Nevertheless, a department spokesman characterized as "baseless" the suggestion that the General Counsel's office blocked access to Department information. The spokesperson continued, "The department goes to great lengths to facilitate information sharing with the IG and GAO. I'm confident that the IG and GAO appreciate that there can be instances when it makes sense to have department counsel involved, especially when it relates to how sensitive information is treated."[233]

---

[226] U.S. GEN. ACCOUNTABILITY OFFICE, HOMELAND SECURITY: MANAGEMENT AND PROGRAMMATIC CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY 23 (2007), http://www.gao.gov/new.items/d07398t.pdf.

[227] *Id.* at 3–4.

[228] Chris Strohm, *Watchdogs say Homeland Security Office has Delayed Probes*, GOV'T EXECUTIVE, Feb. 6, 2007, http://www.govexec.com/dailyfed/0207/020607cdpm1.htm.

[229] *Id.*

[230] *Id.*

[231] *Id.*

[232] *Id.*

[233] *Id.*

V. THE DEPARTMENT'S LINKS TO NEPOTISM AND CRONYISM

For such a young agency, accusations of nepotism and cronyism plague the Department of Homeland Security.[234] The GAO noted that "[a]s DHS strives to fulfill its mission, it faces key challenges in building its credibility as a stable, authoritative, and capable organization and in leveraging private and public assets and information in order to clearly demonstrate the value it can provide."[235]

Although there are numerous examples of appointees that seemingly benefit from cronyism and nepotism—including the Vice-President's son-in-law Philip Perry, the Department's former General Counsel—this article limits its discussion to one of President Bush's more recent and provocative appointments. On January 4, 2006, President Bush appointed Julie L. Myers to the position of Assistant Secretary for U.S. Immigration and Customs Enforcement ("ICE").[236] As ICE employs more than 15,000 individuals, including 6,000 investigators, and has an annual budget in excess of $4 billion, Ms.

---

[234] Shane Harris, *Homeland Security Could Face Transition Problem*, NAT'L J., June 1, 2007, http://www.govexec.com/dailyfed/0607/060107nj1.htm. Individuals possessing questionable qualifications appear to fill important positions within the Department. Consider the following examples. Andrew Maner, a former staffer to President George H.W. Bush, became the Department's Chief Financial Officer. *Id.* Although this is a position that oversees multibillion-dollar budget, Maner could not readily produce evidence of credentials in accounting and finance on his resume. *Id.* Similarly, Douglas Hoelscher, a former White House staffer and Republican campaign aide, was only 28 years old when he became executive director of the Homeland Security Advisory Committee ("HSAC"). *Id.* The HSAC gathers advice on critical issues such as protecting the nation's infrastructure and countering weapons of mass destruction. At the time of his appointment, Hoelscher allegedly did not have management experience, but was acting as the Department's liaison to the White House. *Id.* A Homeland Security spokeswoman observed that Holescher "made sure [that political appointees] were all placed in the office where they were happiest and . . . fit best.") *Id.* At the time that Garcia became the first Assistant Secreatry of Cybersecurity and Telecommunications, Andy Purdy was a two-year contract employee on loan from Carnegie Mellon University. Declan McCullagh, *Homeland Security Fills Top Cybersecurity Post*, CNET NEWS, Sept. 18, 2006, http://www.news.com/Homeland-Security-fills-top-cybersecurity-post/2100-7348_3-6116975.html. Purdy had become the Acting Director of NCSD in the wake of Yoran's sudden resignation. *Id.* Purdy, who has been criticized for taking the job of running a department that awarded at least $19 million in contracts to his university employer this year, was the acting cybersecurity chief. *Id.*

[235] CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 28, at 18.

[236] Department of Homeland Security, Official Biography of Julie L. Myers, http://www.dhs.gov/xabout/structure/biography_0149.shtm.

Myers leads the Department's largest investigative component.[237] Prior to her 2006 appointment, Myers served as special assistant to the President for presidential personnel. She also served as an assistant secretary for Export Enforcement at the Department of Commerce, and was an associate at Mayer, Brown & Platt in Chicago, Illinois.[238]

For several reasons, many found Myers' appointment disconcerting. First, "Given the importance of the position and a history of mismanagement in the immigration service," Congress took the unusual step of statutorily requiring that the Assistant Secretary of the Bureau of Border Security to "have a minimum of 5 years professional experience in law enforcement, and a minimum of 5 years of management."[239] Second, Myers' most relevant prior experience amounted to "managing only 170 employees and a $25 million budget while at the Commerce department."[240] Third, Myers' appointment smacked of cronyism. Myers is the niece of Air Force General Richard B. Myers, the former Chairman of the Joints Chiefs of Staff,[241] and, at the time of the appointment, the wife of John F. Wood, Secretary Chertoff's then Chief of Staff.[242]

Regarding Myers' appointment, Charles Showalter, President of the National Homeland Security Council, a union that represents 7,800 ICE agents, officers and support staff, remarked: "It appears she's got a tremendous amount of experience in money laundering, in banking and the financial areas, [b]ut my question is: Who the hell is going to enforce the immigration laws?"[243] Similarly, during Congressional hearings, Senator Voinovich (R-OH) told Myers that "I'd really like to have [Secretary Chertoff] spend some time with us,

---

[237] *Id.*

[238] *Id.*

[239] Homeland Security Act of 2002, § 442.

[240] Editorial, *Withdraw Myers*, NAT'L REV., Sept. 22, 2005, http://www.nationalreview.com/editorial/editors200509221416.asp.

[241] Michelle Malkin, *Not Another Homeland Security Hack*, JEWISH WORLD REV., Sept. 21, 2005, http://www.jewishworldreview.com/michelle/malkin092105.php3.

[242] *Id.*

[243] Dan Eggen & Spencer S. Hsu, *Immigration Nominee's Credentials Questioned*, WASHI. POST, Sept. 20, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/19/AR2005091901930.html.

telling us personally why he thinks you're qualified for the job, because based on the resume, I don't think you are."[244] Nevertheless, Myers' recess appointment[245] escaped the Senate's full consideration and from January 2006 until November 2008, Myers served as the Assistant Secretary.[246] As one political commentator concluded, the nation recently learned two very valuable lessons regarding homeland security. First, "[i]f you appoint political cronies in a time crisis, you will regret it."[247] Second, "[c]ronyism and national security are a deadly mix."[248] The Department appears to exemplify both of these lessons.

VI. THE DEPARTMENT'S ONGOING LEADERSHIP CRISIS

Representative Thompson once remarked that "Homeland Security was bruised when the country learned that Michael Brown, an Arabian Horse aficionado, was running FEMA."[249] Adding insult to

---

[244] *Id.*

[245] Press Release, Harry Reid, Recess Appointment of Julie Myers Sends Mixed Messages on Border Security (Jan. 5, 2006), *available at* http://democrats.senate.gov/newsroom/record.cfm?id=250483&. The press release stated:

> President Bush's decision to recess appoint Julie L. Myers to the Immigration and Customs Enforcement Bureau sends mixed messages about his real commitment to protect our nation and find a realistic solution to the immigration problems that our nation faces. While the President often talks about the need to protect our borders, Ms. Myers background raises serious questions about her ability to fulfill ICE's important work of preventing the entrance of terrorists and people who want to harm us. I am deeply concerned that the President has handed a key appointment to someone who is not prepared to assume the responsibility of managing such an important agency.

[246] In October 2007, The Senate Judiciary Committee voted to confirm Myers, as did the Senate Homeland Security and Governmental Affairs Committee in September. *See also* Spencer Hsu, *Bush Immigration Chief Julie Myers Out*, Wash. Post, Nov. 5, 2008, http://voices.washingtonpost.com/44/2008/11/05/bush_immigration_chief_julie_m.html.

[247] Malkin, *supra* note 241.

[248] *Id.*

[249] Press Release, H. Committee on Homeland Security, Vacancy Report Finds Homeland Security and Continuity of Government at Risk (July 9, 2007), *available at* http://homeland.house.gov/press/index.asp?ID=237.

injury, the Department's leadership woes are compounded by its employment infrastructure. For example, as of May 1, 2007, the Department maintains 575 executive positions.[250] 138 of these 575 executive positions, or 24%, were vacant.[251] This paucity of senior officials "directly impairs our homeland security and our readiness."[252] Department officials argue that the recent addition of seventy-three senior executive service positions unfairly inflated this number of vacancies.[253] But, some commentators were quick to dismiss the Department's attempt to explain away these deficiencies, noting that 51% (70) of these positions were vacant with no explanation, 44% (61) were under recruitment, 5% (7) tentative or pending appointees.

These vacancies notwithstanding, the year 2009 may challenge the Department in new and unchartered ways. Tuesday, January 20, 2009 is Inauguration Day, a day which represents the first time since its inception that the Department will exist under a presidential administration other than the Bush administration. As of September 2004, the Department employed more than 180,000 individuals, including more than 360 politically appointed, non-career positions.[254] By contrast, the Veterans Affairs Department, the government's second-largest department with over 235,000 employees, has only sixty-four politically appointed, noncareer positions.[255] The Defense Department, the largest government department with over 2.1 million military and civilian employees, maintains only 283 appointed, noncareer jobs.[256] Those 283 jobs include Army, Navy, and Air Force political appointees.[257] Since

---

[250] CRITICAL LEADERSHIP VACANCIES, *supra* note 7, at 3. At least eight agencies and components have a vacancy rate greater than 24% including Office of the Assistant Secretary for Policy (48%), Federal Emergency Management Agency (31%), U.S. Coast Guard (29%), Office of the Assistant Secretary for Intelligence (36%).

[251] *Id.*

[252] *Id.* at 3.

[253] The Department added these positions on March 1, 2007.

[254] Harris, *supra* note 234.

[255] *Id.*

[256] *Id.*

[257] *Id.*

2004, the Department has added political positions more frequently than other large governmental departments.[258]

The Department's organization accounts for much of the anxiety regarding the upcoming transition. Stephen Flynn, a leading expert on the Department, noted that "Any of the other main Cabinet departments have civil servants that step in" as acting officials during a transition period.[259] But, "Homeland Security doesn't have any of those [servants] . . . [a]nd that's extremely unusual."[260] Since its inception, the Department has promoted into senior, or even middle, management positions very few career officials.[261] Consequently, most of the responsibility for running the Department, and its plethora of critical missions, resides in the people who will be walking out the Department's front door as the Bush administration wanes or will leave en masse after the 2008 Presidential election. In short, the "department virtually has no backbench."[262]

Michael P. Jackson, the Department's Deputy Secretary, expressed a commitment to prevent such a leadership meltdown during the transition period between administrations. Jackson confirmed that he was drafting succession plans for "every operational component" of the Department including the top layers of management.[263] Jackson's plan aimed to find talented career, nonpolitical employees that can advance into senior level positions, and then serve in an acting capacity during the transition of presidential administrations.[264] "We've gone throughout the entire organization and looked for people like this to promote. We're trying to nurture a cadre of owners. I am the part-time help at DHS."[265] Nevertheless, Jackson admitted that it is difficult to find and retain quality candidates. "We've had a significant turnover. And that turnover has been below the top-level

---

[258] *Id.*

[259] Harris, *supra* note 234.

[260] *Id.*

[261] *Id.*

[262] *Id.*

[263] *Id.*

[264] Harris, *supra* note 234.

[265] *Id.*

jobs as well . . . [but] I would say we are well beyond the halfway point in what we have to get done."[266]

During a September 5, 2007 hearing, Secretary Chertoff told the House Committee on Homeland Security that as the Bush administration winds down, the Department's senior leadership would remain intact. "I am confident that, again subject to limitations of, you know, presidential pleasure and God's willingness, that the senior leadership team we have in place does intend to stay on, and I think we will shortly be filling the remaining gaps and vacancies."[267] But less than three weeks later, Deputy Secretary Michael Jackson resigned.[268] In a September 24, 2007 e-mail to staff, Jackson wrote, "The simple truth, however, is that after over five years of serving with the President's team, I am compelled to depart for financial reasons that I can no longer ignore."[269] Incidentally, Jackson joined the Department in March 2005, and at the time of his departure, earned $168,000 per year.[270] In a press release, Secretary Chertoff noted that "Michael is the longest serving Deputy Secretary at this department and has devoted enormous energy, talent and thought into making it a stronger, more integrated and mature organization."[271] Jackson further asserted that his departure would not impede the Department's progress. "I have been working very systematically to make sure . . . that the work doesn't drop one bit after my departure . . . . Whoever is my successor is going to inherit a system in good shape."[272]

Nevertheless, the Deputy Secretary's abrupt resignation elicited concern from Representative Thompson. "Secretary Jackson's

---

[266] *Id.*

[267] Chris Strohm, *Resignation of DHS Deputy Prompts Questions on Capitol Hill*, GOV'T EXECUTIVE, Sept. 25, 2007, http://www.govexec.com/dailyfed/0907/092507cdam2.htm.

[268] Eileen Sullivan, *Homeland Security's Jackson Resigns*, USA TODAY, Sept. 24, 2007, http://www.usatoday.com/news/washington/2007-09-24-3552264736_x.htm.

[269] *Id.*

[270] *Id.*

[271] Press Release, Statement by Homeland Security Secretary Michael Chertoff on the Resignation of the Deputy Secretary (Sept. 24, 2007), *available at* http://www.dhs.gov/xnews/releases/pr_1190660057092.shtm.

[272] Rob Margetta, *Pressure Points for the Department of Homeland Security*, CQ WKLY., Oct. 22, 2007, http://public.cq.com/docs/cqw/weeklyreport110-000002609418.html.

departure reaffirms two things we've known for some time, that DHS employees suffer from the lowest morale in the Federal workforce, and that the Department's leadership has more holes than Swiss cheese."[273] Thompson added, "As we near a presidential transition, and with security threats looming around every corner, I'm scared to ask who Secretary Chertoff will turn to now.[274]

Deputy Secretary Jackson responded to Representative Thompson's criticism in kind. In an October 19, 2007 letter to Thompson, Jackson explained that "DHS's leadership team would more fairly be compared to a fully intact wheel of the undisputed king of cheeses, Parmigiano Reggiano, carefully nurtured to maturity and ripe for superlative service."[275] One week later, Thompson sent to the Deputy Secretary another letter that had a tone that was far from humorous. First, Thompson pointed out that if Jackson had accepted the Committee's invitation to testify at the September 18, 2007 hearing titled *The Grades are In!– Is the Department of Homeland Security Measuring Up?*, then Jackson "would have had the opportunity at that time to address many of the issues that [he] now raise[d]."[276] Second, Thompson challenged Jackson's statement that "there is not a single unfilled position among the most senior members of the DHS management team."[277] Specifically, Thompson provided several examples of the "Department's apparent penchant for requiring people to temporarily occupy different positions simultaneously."[278] Third, Thompson rebutted Jackson's claim that

---

[273] Press Release, Thompson Responds to Jackson Resignation (Sept. 24, 2007), *available at* http://hsc.house.gov/press/index.asp?ID=270&SubSection=0&Issue=0&DocumentType=0&PublishDate=0.

[274] *Id.*

[275] Jonathan E. Kaplan, *Dems Say DHS is Swiss Cheese; DHS Says it's Parm*, THE HILL, Nov. 2, 2007, http://thehill.com/leading-the-news/dems-say-dhs-is-swiss-cheese-dhs-says-its-parm-2007-11-02.html.

[276] Letter from Bennie G. Thompson, Ranking Member, H. Comm. on Homeland Security, to Michael Jackson, Deputy Secretary, Department of Homeland Security (Oct. 26, 2007), *available at* http://www.hlswatch.com/sitedocs/thompson-to-jackson.pdf.

[277] *Id.*

[278] *Id.*

the Department is "ripe for superlative service." [279] Thompson explained,

> Let me be clear. I have no doubt that the approximately 180,000 rank-and-file-employees who serve in the Department, while beset by one of the lowest employee satisfaction ratings in the Federal workforce, valiantly strive to deliver superlative service. My concern is that the leadership of the Department does not provide that same level of performance. So, as you depart, I want to provide you with a few examples of my experience with your less than superlative service as the senior level . . . .[280]

Thompson then listed eight such examples of "superlative service."[281] Thompson emphasized that "now is not the time for the Department to rest. The American people deserve a Department that will effectively perform now and in the years ahead. We all deserve much more than we have received for the billions of dollars that the Department has spent." [282] Thompson closed his letter in unforgettable fashion. "So, as you leave, allow me to convey this message to those who remain– to quote Benjamin Franklin, 'Never confuse motion with action.'"[283]

VII. THE DEPARTMENT'S PERVASIVE MISMANAGEMENT

A. THE DEPARTMENT'S PURCHASE CARD DEBACLE

In 2006, the GAO and the Department's Inspector General completed a six-month long audit of Department's use of purchase cards.[284] Because auditors could not distinguish between hurricane-

---

[279] *Id.*

[280] *Id.*

[281] Letter from Thompson, *supra* note 276.

[282] *Id.*

[283] *Id.*

[284] The joint audit progressed from November 2005 through June 2006, examined all purchase card transactions at the Department that occurred from June 13, 2005 through November 12, 2005. U.S. GEN. ACCOUNTABILITY OFFICE, PURCHASE CARDS: CONTROL

related and non-hurricane-related purchases, the auditors evaluated all purchases that occurred during this time frame.[285] The audit's message was clear. Poor oversight plagued the Department. Senator Susan Collins (R-ME) noted, "It seems no matter where we look at Homeland Security, we find a pattern of waste, fraud and abuse."[286] According to Senator Charles Schumer (D-NY), the GAO report showed "yet again that the Department of Homeland Security seems to be sometime[s] run more like a college fraternity house, than an agency meant to protect us from terror."[287]

The report provided a startling description of the Department's financial disarray. Auditors noted that "inadequate staffing and ineffective monitoring contributed to the weak control environment.[288] Despite the presence of nearly 14,000 purchase cards, the Department "failed to assign sufficient resources to manage

---

WEAKNESSES LEAVE DHS HIGHLY VULNERABLE TO FRAUDULENT, IMPROPER, AND ABUSIVE ACTIVITY 2 (2006) [hereinafter PURCHASE CARDS INVITE VULNERABILITY], *available at* http://www.gao.gov/new.items/d06957t.pdf.

[285] *Id.*

[286] Eric Lipton, *Homeland Security Department Is Accused of Credit Card Misuse*, N.Y. TIMES, July 19, 2006, http://www.nytimes.com/2006/07/19/washington/19cards.html?ei=5088&en=5e9000b0261c5602&ex=1310961600&adxnnl=1&partner=rssnyt&emc=rss&adxnnlx=1164294012-DXvgXm9ImuoTtQCqwkhFjA.

The TSA requested that the Defense Contract Audit Agency perform a TSA audit. The results of the audit were shocking. When, in September 2003, the Transportation Security Operations Center opened, the operations center had a 4,200 square foot gym at a cost of $350,000 to accommodate the center's seventy-nine employees. The center also maintained seven kitchens with sub-zero refrigerators, with each refrigerator costing $3,000. The TSA's first director worked in an executive suite that cost $410,000. To celebrate the TSA's first birthday, the agency hosted a party at a cost of $461,000. Sara Kehaulani Goo, *Probe Finds Overspending for TSA Center*, WASH. POST, Apr. 20, 2005, http://www.washingtonpost.com/wp-dyn/articles/A2399-2005Apr19.html. The TSA also paid (1) $1,140 for twenty gallons (or $3.69 per cup) of Starbucks coffee, (2) $1,540 to rent fourteen extension cords at $5 per day for three weeks, (3) $514,210 to rent three tents that flooded in a rain storm, (4) $377,273.75 in unsubstantiated long-distance phone calls, and (5) $4.4 million in "no show" fees for job candidates who did not appear for tests. Scott Higham & Robert O'Harrow Jr., *The High Cost of a Rush to Security*, WASH. POST, June 30, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/06/29/AR2005062903063.html.

[287] Lara Jakes Jordan, *Credit Card Fraud at DHS*, HOMELAND SEC. WKLY., July 19, 2006, http://www.homelandsecurityweekly.com/news/dhs-credit-fraud-071906.

[288] PURCHASE CARDS INVITE VULNERABILITY, *supra* note 284, at 2.

its purchase card program as evidenced by the fact that we found numerous instances where approving officials assumed oversight responsibilities for an excessive number of cardholders."[289] While the GAO guidelines dictate that the ratio of cardholders to approving officials should not exceed seven to one, auditors located three approving Department officials that were each individually responsible for overseeing over thirty cardholders.[290]

This ineffective monitoring also manifested itself in other ways. The report identified the holders of six purchase cards for which the "approving official and the cardholder were the same individual," thereby resulting in a "major conflict of interest."[291] The audit also determined that the Department needlessly distributed to employees purchase cards. The Office of Management and Budget and the United States General Services Administration ("GSA") admonished that "purchase cards should only be issued to individuals who have a documented need to acquire items for the government with the purchase card."[292] But, as of December 13, 2005, the Department actively maintained 2,468 open purchase cards that had not recorded any activity in nearly a year's time.[293] Finding it "difficult to argue that the 2,468 individuals who have not made a single purchase in an entire year have such a need," the report concluded that these accounts "should have been closed to minimize the risk of fraud, waste, and abuse."[294]

These GAO reports also identified several examples of "potentially fraudulent, improper, and abusive or questionable transactions."[295] In one particularly egregious case of purchase card mismanagement,

---

[289] *Id.*

[290] *Id.* The GAO has issued an audit guide prescribing that the ratio of cardholders to approving officials should not exceed seven to one.

[291] *Id.* at 8.

[292] According to the report, federal agency purchase card programs operate under a government wide GSA SmartPay® master contract. Agency purchase card programs must comply with the terms of the contract and task orders under which the agency placed its order for purchase card services. *See* PURCHASE CARDS INVITE VULNERABILITY, *supra* note 284, at 8–9.

[293] *Id.* at 8.

[294] *Id.* at 9.

[295] *Id.* at 3.

FEMA paid a vendor $208,000 to deliver twenty flat-bottom boats needed for relief operations in New Orleans.[296] Although this price included the motors and trailers for the boat, the purchase price was twice the normal retail price.[297] Because the vendor did not physically possess the boats, the vendor used the FEMA purchase card account number to purchase the boats from various other retailers.[298] The vendor used the card number to make two unauthorized payments to one retailer for six of the twenty boats, which payments totaled about $30,000.[299] In the end, FEMA had only eight of the twenty boats in its property records and could not locate the other twelve boats,[300] and the GAO estimated that the vendor used this unauthorized FEMA transaction to collect nearly $150,000, including the profit that the unscrupulous vendor acquired without paying the trusting retailer.[301]

These GAO reports collectively concluded that the Department had not effectively managed its purchase card program, or the policies that govern that program. The examiners could not examine over 10,339 transactions selected for audit, because Department cardholders had not submitted the required supporting documentation.[302] Consequently, based on the audit's sample of purchases using Department purchase cards, the GAO "estimated that 45% did not have prior written authorization, 8% did not provide required sales documentation, 63% did not have evidence that the goods or services were actually received, and 53% did not give priority to required or preferred vendors (designated sources).[303] This lack of oversight and control "allowed potentially fraudulent, improper, and

---

[296] *Id.* at 21.

[297] *Id.*

[298] *Id.*

[299] PURCHASE CARDS INVITE VULNERABILITY, *supra* note 284, at 21.

[300] *Id.*

[301] *Id.* Although the vendor billed FEMA for all twenty of the boats, the vendor failed to pay a retailer that provided eleven of the twenty boats. Because the retailer believed that the vendor was a FEMA representative, the retailer provided the vendor with the boats without requiring an up-front payment. The retailer has since reported the eleven boats as stolen and has not provided the vendor title to the boats.

[302] *Id.* at 10.

[303] *Id.* at 4.

abusive or questionable usage of these purchase cards to go undetected."[304]

The GAO audit likewise demonstrated that the Department exercised poor control over the accountable property that the Department acquired using purchase cards. [305] Auditors closely examined the following FEMA purchases: (1) two hundred laptops for $300,000, (2) twenty flat bottom boats for $177,000, (3) one hundred printers for $84,000, and (4) twenty-five GPS units for $18,000.[306] Auditors also examined the Coast Guard's purchase of three laptops for $13,000.[307] During the investigation, auditors could not locate more than 107 of the 203 computers, twelve of the twenty flat-bottom boats, twenty-two of the one hundred printers, and two of the twenty-five GPS units.[308] The missing computers, GPS units, and printers purchased by FEMA cost the Department approximately $170,000.[309]

B. THE DEPARTMENT'S INCREDIBLE CONTRACTING WOES

In another report, the GAO focused on the Department's *Ongoing Challenges in Creating an Effective Acquisition Organization.* [310] Although the report recognized that interagency contracts provide the Department with the "advantages of timeliness and efficiency," the GAO cautioned that certain risk accompanied the improperly managed contracts.[311] Having spent over $6.5 billion on interagency

---

[304] *Id.* at 30.

[305] The Department's Personal Property Management Directive 565 defines accountable property as personal property with an initial acquisition cost at or above a specific threshold, and items designated as sensitive. These items are to be recorded in the organization's automated control system. PURCHASE CARDS INVITE VULNERABILITY, *supra* note 284, at 18.

[306] *Id.* at 19.

[307] *Id.*

[308] *Id.*

[309] *Id.*

[310] U.S. GEN. ACCOUNTABILITY OFFICE, DEPARTMENT OF HOMELAND SECURITY: ONGOING CHALLENGES IN CREATING AN EFFECTIVE ACQUISITION ORGANIZATION 1 (2007) [hereinafter ONGOING CHALLENGES IN ACQUISITION], *available at* http://www.gao.gov/new.items/d07948t.pdf.

[311] *Id.* at 8.

contracts during the fiscal year 2005, the GAO concluded that the Department "did not systematically monitor or assess its use of interagency contracts to determine whether this method provides good outcomes for the department."[312]

Part of the Department's problem is the Department itself. The report explains that of the twenty-two components that became part of the Department, seven came with their own procurement support.[313] One year later, in January 2004, the Department created an eighth office—the Office of Procurement Operations—to provide to a variety of Department components procurement support.[314] In December 2005, the Chief Procurement Office ("CPO") established a department wide acquisition oversight program.[315] The Department hoped that the program would provide comprehensive oversight of each component's acquisitions, and disseminate throughout the Department successful acquisition management strategies.[316] Although the GAO reported some progress "in increasing staff to authorized levels," the report concluded that the CPO "lacks the authority needed to ensure the department's components comply with its procurement policies and procedures such as the acquisitions oversight program."[317]

Prompted by this series of scathing GAO reports, the Senate Committee on Homeland Security and Governmental Affairs held a hearing titled *Is DHS Too Dependent on Contractors to Do the Government's Work?* On October 17, 2007, in his opening remarks, Senator Joseph Lieberman (I-CT) noted that while the GAO refrained from making any conclusion regarding whether the Department improperly allowed contractors to perform inherently governmental work, the GAO determined that the Department's oversight plans lacked "specific measures for assessing contractor performance."[318]

---

[312] *Id.*

[313] *Id.* at 3.

[314] *Id.*

[315] ONGOING CHALLENGES IN ACQUISITION, *supra* note 310, at 3.

[316] *Id.*

[317] *Id.* at 6.

[318] *Is DHS Too Dependent on Contractors to Do the Government's Work?: Hearing Before S. Comm. on Homeland Security and Governmental Affairs*, 110th Cong. (2007) (statement of Joseph I. Lieberman, Chairman, S. Comm. on Homeland Security and

Lieberman then described some of the questionable uses of contractors. First, the Coast guard hired a contractor to aid in the management of its competitive outsourcing program.[319] In other words, the Coast Guard hired a contractor to help the Coast Guard determine whether the Coast Guard should use contractors. Second, the Department awarded one contractor a $42.4 million contract to support the Information Analysis and Infrastructure Protection Directorate.[320] Although the contract covered fifty-eight distinct tasks, the Department assigned only one Department employee to provide the contracting officer with relevant support.[321] Senator Lieberman also noted that the "GAO's report leads us to question whether DHS is really in control of these activities, or whether the Department has been rubber-stamping too many decisions made by contractors."[322] In short, the Senator concluded that the Department's "heavy reliance on contractors" may cause the Department to "lose some of their critical ability to think and act on its own for the American people."[323]

Representative Henry Waxman (D-CA) echoed Senator Lieberman's sentiments. Waxman explained that "federal procurement decisions affect the lives of every American. Contractors have become a 'shadow government,' an enormous workforce of hundreds of thousands of people who perform a vast array of government functions."[324] In a 2006 report titled *Dollars, Not Sense:*

Governmental Affairs), *available at* http://hsgac.senate.gov/public/_files/101707JILOpen.pdf.

[319] *Id.*

[320] *Id.*

[321] *Id.*

[322] *Id.*

[323] *Is DHS Too Dependent on Contractors to Do the Government's Work?*, *supra* note 318. In her opening statement, Senator Susan Collins quoted a handbook published by the Office of Personnel Management. "Managers need to keep in mind that when they contract out . . . they are contracting out the *work*, not the *accountability*." *Is DHS Too Dependent on Contractors to Do the Government's Work? Before the S. Subcomm. on Homeland Security and Governmental Affairs*, 110th Cong. (2007) (statement of Susan M. Collins, Ranking Member, S. Comm. on Homeland Security and Governmental Affairs), *available at* http://hsgac.senate.gov/public/_files/101707SMCOpen.pdf.

[324] Rep. Henry A. Waxman, Chairman, H. Comm. on Oversight and Government Reform, Remarks at the Center for American Progress' Forum on a Return to Competitive Contracting (May 14, 2007), *available at*

Government Contracting under the Bush Administration, Waxman explained that federal contracting is the fastest growing aspect of the government's discretionary budget.[325] Waxman complained that when asked at a February 2007 hearing, the Department could not determine how many contractors it employed.[326] Because the Department's "lack of accountability and oversight is an invitation to abuse," the House Oversight Committee launched an investigation into the Department's use of contractors.[327] Waxman explained, "While government contractors are getting rich, the taxpayers are getting soaked. Billions of dollars are being squandered while our nation's most pressing needs have gone unmet. Major government initiatives . . . have been undermined by wasteful spending on federal contracts."[328]

In an October 25, 2005 letter to Representative Tom Davis (R-VA), Waxman pleaded for the Committee to "investigate reports of egregious waste under contracts awarded and administered by the Department of Homeland Security."[329] Waxman referred the Committee's attention to a *Washington Post* article that divulged the findings of a Pentagon audit.[330] The Pentagon audit examined a $1 billion contract between Unisys and the Transportation Security Administration ("TSA") to upgrade the computer networks serving the nation's airports. Auditors discovered that Unisys may have

---

htttp://oversight.house.gov/documents/20070515121402.pdf. In a 2006 report titled *Dollars, Not Sense: Government Contracting under the Bush Administration*, Waxman explained that federal contracting is the fastest growing aspect of the government's discretionary budget. *See* HOUSE COMMITTEE ON GOVERNMENT REFORM, DOLLARS, NOT SENSE: GOVERNMENT CONTRACTING UNDER THE BUSH ADMINISTRATION i (2006), http://oversight.house.gov/documents/20061211100757-98364.pdf.

[325] *Id.*

[326] Waxman, *supra* note 324.

[327] *Id.*

[328] *Id.*

[329] Letter from Henry Waxman, Ranking Minority Member, H. Comm. on Government Reform, to Tom Davis, Chairman, H. Comm. on Government Reform (Oct. 25, 2005), *available at* http://oversight.house.gov/documents/20051025100329-39397.pdf.

[330] Robert O'Harrow Jr. & Scott Higham, *Contractor Accused Of Overbilling U.S; Technology Company Hired After 9/11 Charged Too Much for Labor, Audit Says*, WASH. POST, Oct. 23, 2005, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/10/22/AR2005102201437_pf.html.

"overbilled taxpayers for as much as 171,000 hours' worth of labor and overtime by charging up to $131 an hour for employees who were paid less than half that amount."[331] In closing, Waxman delivered this ultimatum. "Unless we radically change our approach toward the Homeland Security Department, we will not fulfill our constitutional obligation to conduct oversight and to protect the taxpayer from waste, fraud, and abuse."[332]

Others share Congress' concerns. Professor Steven L. Schooner, the Co-Director of the Government Procurement Program at the George Washington University Law School, also testified at the October 2007 hearing. Schooner explained that as the nation's procurement system "struggled throughout this decade, Congress has been quick to call for more auditors and inspectors general to scrutinize contracting."[333] While characterizing this reaction as a "responsible gesture," Schooner believes it was not enough.[334] Schooner concluded that the Department does not have "meaningful short-term alternatives for escaping its current predicament . . . . Only serious, long term, far reaching personnel reforms can, in any meaningful manner, begin to reverse the current trend."[335]

In short, mismanagement and lack of oversight plague the Department. As a result, the American taxpayers are forced to pay, literally, for the Department's mismanagement. Reports like these

---

[331] According to the audit, "Unisys billed taxpayers $131.12 an hour for a technical writer who should have made no more than $46.43. The extra money was generally not passed along to the employees but was kept by the company." Similarly, Pentagon auditors concluded that "Unisys and its subcontractors billed the government for 24,982 hours' worth of overtime that was not permitted under the contract," and that the overtime charges "appeared to represent '100 percent profit to Unisys.'" *Id.*

[332] Waxman Letter, *supra* note 329. Recently, Unisys has also been implicated in misconduct regarding a series of cyber attacks. According to information uncovered by the House Committee on Homeland Security, Unisys's failure to properly install and monitor the Department's information technology networks. *See* Ellen Nakashima & Brian Krebs, *Contractor Blamed in DHS Data Breaches*, WASH. POST, Sept. 24, 2007, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html.

[333] *Is DHS Too Dependent on Contractors to Do the Government's Work?: Hearing Before the S. Subcomm. on Homeland Security and Governmental Affairs*, 110th Cong. (2007) (statement of Steve L. Schooner, Co-Director, Government Procurement Law Program), *available at* http://hsgac.senate.gov/public/_files/101707Schooner.pdf.

[334] *Id.*

[335] *Id.*

prompted Senator Lieberman to ask, "How can the Department possibly protect the nation's critical cyber-structure if it cannot keep its own house in order?"[336]

VII. CONCLUSION

The *National Strategy to Secure Cyberspace* recognized that "[g]overnment alone cannot sufficiently secure cyberspace,"[337] and that "[n]o single strategy can completely eliminate cyberspace vulnerabilities and their associated threats."[338] Furthermore, the *National Strategy* advised that because "the private sector is best equipped and structured to respond to an evolving cyber threat," the "public-private engagement" is an indispensable component of the nation's strategic efforts to secure cyberspace.[339] Similarly, the *2005 Report to the President* recognized the need for the right people to be in the right places at the right time. "Improving the Nation's cybersecurity posture requires highly trained people to develop, deploy, and incorporate new cybersecurity products and practices."[340]

---

[336] Press Release, Senator Joseph Lieberman, DHS Is Failing in Its Cyber-Security Responsibilities (July 11, 2005), *available at* http://lieberman.senate.gov/newsroom/release.cfm?id=240394.

[337] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 2 (2003), http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf. *See also* Corey McKenna, *Chertoff Calls for Public-Private Cooperation on Cybersecurity*, GOV'T EXECUTIVE, Aug. 2, 2005, http://www.govtech.com/gt/96147?topic=117671 (quoting Secretary Chertoff, "Security, even cyber security, cannot take the form of government dictates, but must be the product of strong partnership work and disciplined collaboration.").

[338] THE NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 337, at 10.

[339] *Id.*

[340] *See* PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE, CYBER SECURITY: A CRISIS OF PRIORITIZATION 3 (2005) [hereinafter PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE], *available at* http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf. One industry insider commented:

> One important objective of any sharing activities, therefore, should be to shorten the time it takes for the defenders to respond to new attacks. That requires not only strong computer security technical skills but also sharing of knowledge among the "good guys and gals" that is at least as effective as the sharing that goes on among those who would do us harm.

Given the magnitude of this task, the number of qualified individuals involved in the Department's efforts is far too small.[341] The report concluded:

> The Federal government should intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the Federal government should increase and stabilize the funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.[342]

But, the Department has not accomplished these goals. Despite well-meaning intentions, there "continues to be a lack of leadership, hard work and execution when it comes to securing the information infrastructure."[343]

Even if the Department finds (and retains) these qualified individuals, will it be enough? Will the Department allow individuals to do what is necessary in the face of a catastrophe? The protection of this Nation's cyber infrastructure is critical for its survival. Yes, the obstacles are intimidating, but, the "American people are tired of hearing that getting a 'D' is a security improvement."[344] The nation's enemies "use[] the Internet to great effect to share information. We need to be at least as effective."[345] As the GAO reports seem to

---

See Securing Our Infrastructure: Private/Public Information Sharing: Hearing Before the S. Comm. on Governmental Affairs, 107th Cong. (2002) (statement of Alan Paller, Director of Research, The SANS Institute) [hereinafter *Securing Our Infrastructure*], *available at* http://www.senate.gov/~govt-aff/050802paller.pdf.

[341] PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE, *supra* note 340, at 3.

[342] *Id.*

[343] "We are not seeking to condemn the government or those currently involved in cybersecurity."

[344] *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security: Hearing Before the H. Comm. of Homeland Security*, 110th Cong. (2007) (Statement of Rep. Bennie G. Thompson, Chairman), *available at* http://hsc.house.gov/SiteDocuments/20070620144350-15564.pdf.

[345] *Securing Our Infrastructure*, *supra* note 340.

indicate that the "[r]estructuing the federal bureaucracy [was] the wrong approach [because] [t]he creation of the massive Department of Homeland Security has produced no efficiencies or synergy and arguably has weakened each of the component parts."[346]

Attacks on the nation's cybersecurity are constant and virulent. The federal government has tapped the Department to patrol and protect the Nation's cyber infrastructure. But, as explained in detail, waste, inefficiency, and mismanagement plague the Department and stymie the federal government's legitimate attempts to provide security. This ineffectiveness leads to the question– who, or what, deserves the blame? The answer to that question is not easily answered, and this article addresses only a few of the many issues that factor into the cyber equation. Therefore, any solution for redressing the Department's inadequacies must streamline the mechanism by which the Department identifies and addresses cyber threats.

Napoleon Bonaparte once said, "Take time to deliberate, but when the time for action has arrived, stop thinking and go in." The security of the Nation's cyber infrastructure is tenuous, and to echo the industry's battle cry: "the time for action is now. We have moved beyond the discussion and planning phase and have identified concrete actions that can be taken by the administration to immediately improve the security of our nation's cyber systems."[347] When it comes to securing the Nation's cyber infrastructure, the words of the Jedi Master Yoda resonate: "Do, or do not. There is no try."[348]

---

346 Brittany L. Dorn, *Does Nation Need New Super-Agency?*, HARTFORD COURANT, July 20, 2007, at B5, *available at* http://www.topix.net/content/trb/2007/07/does-nation-need-new-super-agency.

347 Corey McKenna, *Industry Group Calls on Federal Government to Strengthen Cyber Security*, GOV'T TECH., Dec. 13, 2004, http://www.govtech.com/gt/92458?topic=117688.

348 THE EMPIRE STRIKES BACK (20th Century Fox 1980).